Le traitement de données dans le cadre des communications électroniques

Rosier, Karen

Published in:
Vie privée et données à caractère personnel

Publication date:
2013

Document Version
le PDF de l'éditeur

CHAPITRE 5.1.
INTRODUCTION

Karen ROSIER[1]

1. Objet de la présente contribution

La protection des données à caractère personnel s'est invitée dans le secteur des communications électroniques depuis de nombreuses années. Il est vrai que ce secteur touche à des aspects extrêmement sensibles du domaine de la protection de la vie privée et des données à caractère personnel. Il suffit de penser à la quantité d'informations transitant par les réseaux de communications électroniques ou qui peut être révélée par les données relatives à l'utilisation de ceux-ci.

Si les communications électroniques sont protégées par l'article.8 CEDH et l'article 22 de la Constitution qui consacrent le droit au respect de la vie privée[2], nous nous pencherons dans le cadre de cette contribution sur certaines dispositions d'une loi particulière qui organise une protection dans ce secteur. Il s'agit de la loi du 13 juin 2005 relative aux communications électroniques et plus spécifiquement des articles 122 et suivants de cette loi qui forment la section intitulée « Secret des communications, traitement des données et protection de la vie privée »[3].

Nous nous proposons d'analyser plus spécifiquement les articles 122 à 129 de la loi. Ces dispositions concernent les conditions dans lesquelles on peut prendre connaissance et traiter des données relatives à des communications électroniques. Il nous apparaît qu'elles forment le cœur de la réglementation du traitement des données à caractère personnel dans le secteur des communications électroniques. Toutefois, le fait que la réglementation s'ancre dans une loi qui entend régir de manière générale une grande partie du secteur des communications électroniques a un impact sur la

1. L'auteur tient à remercier Mme Cécile de Terwangne, Professeur à la Faculté de droit de l'Université de Namur, ainsi que M. Robert Queck, Maître de conférences à l'Université de Namur et M. Maxime Piron, chercheur au CRIDS, pour leurs judicieux conseils.
2. Voy., notamment, Cour eur. D.H., arrêt Halford c. Royaume-Uni, 25 juin 1997, req. n° 20605/92 ; Cour eur. D.H., arrêt Copland c. Royaume-Uni, 3 avril 2007, req. n° 62617/00.
3. Et qui forme la section 2 du chapitre III du titre IV de la loi du 13 juin 2005.

portée des dispositions. Nous nous en rendrons compte en tentant de définir leur champ d'application matériel, territorial et personnel au sein du chapitre 5.2., *infra.*

Les dispositions qui seront analysées s'articulent autour d'un principe qui est celui du secret des communications électroniques consacré à l'article 124 de la loi et qui prend la forme d'une interdiction de prendre connaissance des informations transmises par le biais de communications électroniques, des données de communications et de l'identité des personnes concernées par la communication. Concrètement, cette disposition vise à protéger des données qui concernent les courriels, les communications téléphoniques, les SMS, les MMS, les données de connexion à l'Internet, par exemple. Des exceptions à ce principe sont envisagées aux articles 125 et 128 de la loi. Nous y reviendrons sous le chapitre 5.3, *infra.*

La loi réglemente par ailleurs spécifiquement les traitements qui peuvent être effectués par les personnes impliquées dans la fourniture des services de communications. Ainsi l'article 122 de la loi entend-il autoriser et encadrer certains traitements effectués par les opérateurs sur les données dites « de trafic » qui servent à la transmission ou à la facturation des services de communications électroniques. La technologie évoluant, il a également été nécessaire de se pencher sur le sort d'un autre type de données qui peuvent être générées par les communications électroniques : celles dites « de localisation », qui révèlent l'emplacement géographique d'un terminal (GSM, GPS, PC portable, etc.) et, par extension, celui de son utilisateur. La loi du 13 juin 2005 régit spécifiquement, en son article 123, dans quelles conditions et à quelles finalités des opérateurs ou des tiers qui fournissent des services faisant usage de ces données peuvent les traiter. Ces deux dispositions seront analysées sous le chapitre 5.4. Il y sera également question des articles 126 et 127 de la loi qui, nous le verrons, mettent les opérateurs et d'autres fournisseurs de services de communications à contribution pour conserver des données et collaborer avec certaines autorités, notamment les autorités judiciaires dans le cadre d'enquêtes pénales.

Nous nous pencherons ensuite, dans le chapitre 5.5, sur l'article 129 de la loi du 13 juin 2005 qui traite d'un autre aspect du droit au respect de la vie privée et de la protection des données : celui de l'utilisation de logiciels espions ou de fichiers tels que des *cookies* qui peuvent révéler des informations sur l'usage par l'internaute des services de communications électroniques.

Nous n'aborderons donc pas les autres dispositions de la section de la loi qui règlent notamment certains aspects de la fourniture des services de téléphonie (l'identification des lignes appelantes et appelées, le renvoi automatique des appels vers le terminal d'un abonné, ainsi que l'insertion des numéros de téléphone dans des annuaires).

Avant de procéder à l'analyse des dispositions précitées, il nous paraît indispensable d'en situer l'origine en identifiant les directives européennes qu'elles sont censées transposer. Nous nous y attacherons dans le point 2 ci-dessous.

L'introduction de cette problématique ne serait pas complète sans se pencher sur les interactions qui existent entre la loi du 13 juin 2005 et la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. En effet, comme l'annonce d'ailleurs l'intitulé de cette contribution, les dispositions analysées participent au cadre légal de la protection des données à caractère personnel. Il nous semble dès lors opportun de cerner d'emblée comment les dispositions des deux lois s'articulent entre elles et quelles difficultés peuvent résulter, le cas échéant, de l'application cumulative de ces textes. Nous traiterons de ces questions sous le point 3.

2. Situation des dispositions analysées par rapport au cadre européen

Les dispositions de la loi du 13 juin 2005 relative aux communications électroniques, qui traitent des aspects de la vie privée, transposent la directive (CE) n° 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[1]. Cette directive fait partie d'un paquet de cinq directives (« Paquet Télécom ») qui était destiné à réformer le cadre réglementaire régissant les services et réseaux de communications électroniques dans la Communauté. Ce processus réformateur avait été initié en 1999, tandis que les discussions propres à la directive (CE) n° 2002/58 ont débuté, quant à elles, en juillet 2000. Le nouveau cadre juridique devait permettre d'assurer une réglementation analogue et un même niveau de protection des consommateurs pour tous les services indépendamment de la technologie utilisée pour les fournir[2].

La directive (CE) n° 2002/58 remplace la directive (CE) n° 97/66 du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Elle a principalement pour objectif d'étendre le champ d'application de la directive (CE) n° 97/66 aux « communications électroniques », notion sur laquelle nous reviendrons au sein des chapitres 5.2 et 5.3 En effet, dès son adoption, la directive (CE) n° 97/66 était déjà dépassée par la technologie existante, puisqu'elle se cantonnait, comme le suggé-

1. Directive (CE) n° 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ou « directive vie privée et communication ».
2. J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (anciennement revue Ubiquité)*, 2003, p. 7.

raient son intitulé et la terminologie utilisée, au secteur des télécommunications là où Internet et les nouveaux moyens de communication y relatifs avaient fait leur apparition. Ceci explique que la terminologie utilisée dans la directive (CE) n° 2002/58 se veuille neutre du point de vue technologique[1].

La loi du 13 juin 2005 sera adoptée pour transposer en droit belge le Paquet Télécom évoqué *supra*, dont la directive (CE) n° 2002/58. Elle abrogera en grande partie la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (à laquelle il était fréquemment fait référence sous les termes « loi Télécom » ou « loi Belgacom »). Parmi les dispositions que nous nous proposons d'analyser, il s'en trouve certaines qui existaient déjà sous une forme plus ou moins similaire dans la loi Télécom. Nous pensons en particulier aux articles 109*ter*D et 109*ter*E qui régissaient le secret des communications électroniques et qui sont « remplacés » par les articles 124 et 125 de la loi du 13 juin 2005. Nous ne reviendrons pas sur les dispositions anciennement applicables sauf dans la mesure où elles permettraient de donner un éclairage utile sur la portée des dispositions actuellement en vigueur.

Il convient également de noter qu'en 2006, la réglementation au niveau européen a été complétée par la directive (CE) n° 2006/24[2] sur la rétention des données[3]. Cette directive vise à imposer aux fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications de conserver certaines données de communications en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre[4]. Nous verrons que la transposition de cette directive en droit belge est encore incomplète à ce jour[5].

Enfin, des modifications au texte de la directive (CE) n° 2002/58 ont été apportées par la directive (CE) n° 2009/136 du 25 novembre 2009[6], ce qui a entraîné quelques adaptations à la loi du 13 juin 2005 par le biais de deux lois, dont celle du 10 juillet 2012[7] qui a modifié le texte de l'article 129 que nous serons amenés à analyser[8].

---

1. J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (anciennement revue* Ubiquité), 2003, pp. 7 et 8.
2. Directive (CE) n° 2006/24 du Parlement et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive (CE) n° 2002/58.
3. La possibilité d'imposer la conservation des données était déjà envisagée sur la base de l'article 15.1 de la directive (CE) n° 2002/58. La directive (CE) n° 2006/24 vient compléter le cadre de la réglementation sur ce point.
4. Voy. article 1er, alinéa 1er, de la directive (CE) n° 2006/24. Pour un commentaire de cette directive, voy. J. Schultze-Melling, « Directive 2006/24/CE (Data Retention Directive) », *in Concise European IT Law*, 2e éd., Kluwer Law International, 2010, pp. 243 et s.
5. *Cf.* Chapitre 5.3., *infra*.
6. Modifiant la directive (CE) n° 2002/22 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive (CE) n° 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.
7. Loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques.
8. Une première loi du 31 mai 2011 portant des dispositions diverses en matière de télécommunications avait transposé une partie de la directive.

3. Liens avec la législation sur la protection des données à caractère personnel

3.1. Les directives (CE) n^{os} 2002/58 et 2006/24 dans le cadre de la réglementation sur le traitement personnel

La directive (CE) n° 2002/58 et la directive (CE) n° 2006/24 ont vocation à régir certains aspects du traitement de données à caractère personnel dans le cadre du secteur des communications électroniques.

Au niveau européen, le texte de référence en la matière est la directive (CE) n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette directive a été transposée en droit belge par une adaptation substantielle de la loi du 8 décembre 1992 en 1998[1].

Les dispositions de la loi du 13 juin 2005 que nous analyserons font donc partie de la législation sur les données à caractère personnel. Il nous apparaît dès lors que se pose la question de savoir comment articuler exactement la loi du 8 décembre 1992 et la loi du 13 juin 2005[2]. Nous abordons cette question dans la section suivante.

3.2. L'articulation entre la loi du 13 juin 2005 et la loi du 8 décembre 1992

Tout d'abord, on peut se demander s'il faut considérer que les dispositions de la loi du 13 juin 2005 qui entendent régir spécifiquement le traitement de certaines données (nous pensons en particulier aux données de trafic ou aux données de localisation) ne s'appliquent que dans la mesure où ces données constituent des données à caractère personnel.

On constate à cet égard un certain hermétisme dans les deux lois en ce qui concerne la définition des concepts utilisés respectivement par chacune d'elles pour édicter les règles matérielles applicables.

---

1. *Cf.* la loi du 11 décembre 1998 transposant la directive (CE) n° 95/46 du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données. Les modifications apportées par la loi du 11 décembre 2008 à la loi du 8 décembre 1992 ne sont cependant entrées en vigueur qu'en 2001. L'entrée en vigueur était en effet subordonnée à l'adoption de mesures d'exécution dans un arrêté royal qui ne fut promulgué que le 13 février 2001.
2. Pour une analyse des liens existant entre les directives (CE) n^{os} 95/46 et 2002/58, voy. K. Rosier, « La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative au traitement des données à caractère personnel : comment les (ré)concilier ? », *in Défis du droit à la protection de la vie privée*, Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, pp. 328 à 352.

Ainsi, dans la loi du 13 juin 2005, il est fait référence non pas à des « données à caractère personnel »[1] qui sont seules visées par la loi du 8 décembre 1992, mais à des « données de trafic » et à des « données de localisation ».

La « donnée de trafic » est définie comme « toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication »[2]. La « donnée de localisation » s'entend, quant à elle, de « toute donnée traitée dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communications électroniques accessible au public »[3].

S'il n'est pas explicitement question de « données à caractère personnel », les travaux préparatoires de la loi du 13 juin 2005 font, quant à eux, toutefois clairement référence à cette notion[4] de sorte qu'il nous paraît qu'il faut en conclure que, pour que des données soient considérées comme des données de trafic ou des données de localisation, elles doivent constituer des données à caractère personnel.

Cette orientation nous semble cohérente par rapport à ce que l'on peut déduire des textes des directives que ces deux lois transposent. Si l'on se réfère à la directive (CE) n° 2002/58, on constate, en effet, qu'un lien est fait entre les deux législations, ne serait-ce que dans l'intitulé de la directive (« concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques »). Il subsistait toutefois un doute quant à la portée de ce lien[5]. Le considérant 51 de la directive (CE) n° 2009/136 tend à lever ce doute et revient sur l'objectif poursuivi par la directive (CE) n° 2002/58 en ces termes : « la directive 2002/58/CE (directive "vie privée et communications électroniques") prévoit l'harmonisation des dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et des libertés fondamentaux, notamment du droit à la vie privée et du droit à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques [...] ».

---

1. Qui, au sens de l'article 1er, § 1er, de la loi du 8 décembre 1992 s'entendent comme étant « toute information concernant une personne physique identifiée ou identifiable, désignée ci-après "personne concernée" », tandis qu'il est précisé dans cette même disposition qu'« est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».
2. Article 2, 6°, de la loi du 13 juin 2005.
3. Article 2, 7°, de la loi du 13 juin 2005.
4. Le commentaire de l'article 122, qui portait initialement le n° 131 dans le projet initial, précise que « [l]'article 131 pose le principe selon lequel les données relatives au trafic concernant des abonnés doivent être supprimées ou rendues anonymes dès qu'elles ne sont plus nécessaires pour la transmission de la communication. Ceci est tout à fait conforme à l'un des principaux objectifs de la directive vie privée, qui consiste à réduire au minimum le traitement des données à caractère personnel et à utiliser des données anonymes ou pseudonymes lorsque c'est possible » (projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, sess. 2003-2007, n° 1425-01/1426-01, p. 73).
5. J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (anciennement revue Ubiquité)*, 2003, pp. 10 à 12.

Ceci nous amène à une seconde interrogation. On peut, en effet, se demander comment combiner les dispositions des deux lois, celles du 8 décembre 1992 et du 13 juin 2005 qui, on l'a vu, régissent toutes deux le traitement de données à caractère personnel.

Sur ce point également, le texte de la loi du 13 juin 2005 n'est pas très précis. Dans plusieurs dispositions, il mentionne que la règle prévue s'applique « sans préjudice de la loi du 8 décembre 1992 »[1]. Ainsi en est-il à l'article 122, § 2, qui prévoit que certaines informations doivent être portées à la connaissance de l'abonné ou de l'utilisateur final « sans préjudice de l'application de la loi du 8 décembre 1992 ». Les travaux préparatoires indiquent à cet égard que « [l]e traitement est autorisé à condition que les abonnés, et le cas échéant, les utilisateurs finals, soient informés, avant le traitement, des informations définies à l'alinéa 2 du paragraphe 2. Cependant, cet alinéa est d'application "sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée et à l'égard des traitements de données à caractère personnel", et ce pour attirer l'attention sur le fait que l'opérateur ne doit pas uniquement respecter la loi spécifique (pour lui) actuelle, mais aussi la loi générale du 8 décembre 1992 pour tous les points qui ne sont pas réglés dans cette loi (comme par exemple le droit d'accès aux données, les obligations du responsable du traitement, etc.) »[2].
On en déduit donc que la loi du 8 décembre 1992 ne trouve à s'appliquer que pour les aspects non spécifiquement réglés par la loi du 13 juin 2005.
À nouveau cette solution nous semble conforme avec ce qui est prévu au niveau de la directive (CE) n° 2002/58. Selon le considérant 10 de cette directive, les dispositions de la directive (CE) n° 95/46 s'appliquent pour toutes les questions relatives à la protection des droits et libertés fondamentaux dans le secteur des communications électroniques qui ne sont pas spécifiquement couverts par les dispositions de la directive (CE) n° 2002/58, y compris en ce qui concerne les obligations du responsable du traitement et les droits des individus.

Concrètement toutefois, cette solution appelle des précisions pour certains aspects de la protection des données.

On pourrait se demander si les seules informations à transmettre aux personnes concernées désignées par la loi du 13 juin 2005 sont celles prévues par cette loi ou s'il y a lieu d'imposer la fourniture d'autres informations en se fondant sur l'article 9 de la loi du 8 décembre 1992 qui définit les informations à fournir à la personne concernée par un responsable de traitement. La deuxième interprétation nous paraît devoir être retenue vu le fait que la loi du 8 décembre 1992 reste d'application. Ainsi, dans le cadre du traitement de données relatives aux communications électroniques,

1. Voy. les articles 122, § 2, 123, § 1er, 128 et 129 de la loi du 13 juin 2005.
2. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, sess. 2003-2007, n° 1425-01/1426-01, p. 74.

les personnes concernées devraient être informées de l'identité du responsable du traitement, des finalités du traitement et également de toute autre information nécessaire pour assurer la transparence et la loyauté de celui-ci en application des dispositions de la loi du 8 décembre 1992. Il serait effectivement paradoxal que l'information soit réduite à ce qui est prévu dans la loi du 13 juin 2005 dans l'hypothèse où les données traitées seraient des données relatives au trafic ou des données de localisation par exemple.

Une autre difficulté qui revient de manière récurrente dans les articles que nous analyserons réside dans l'identification de la personne à informer.

Dans les articles 122, 123 et 129 de la loi du 13 juin 2005 sont utilisés des concepts différents de celui de la « personne concernée » spécifique à la loi du 8 décembre 1992, pour désigner les personnes qui doivent recevoir les informations relatives aux traitements, et, dans certains cas, y consentir. On retrouve, dans ces dispositions, des références à l'abonné qui est « toute personne physique ou morale qui utilise un service de communications électroniques en exécution d'un contrat passé avec un opérateur ». Il s'agit donc du cocontractant. Mais ce cocontractant n'est pas toujours la personne qui utilisera *in fine* le service et adressera ou recevra des communications électroniques via ce service. C'est pourquoi la loi vise en certaines dispositions l'utilisateur[1] ou l'utilisateur final[2].

Dans plusieurs avis de la Commission de la protection de la vie privée (C.P.V.P.)[3] et du Groupe de l'article 29[4], ces autorités se sont prononcées pour que, lorsqu'il est question d'informer ou de solliciter le consentement d'une personne dans le cadre de l'application des dispositions régissant le traitement de données dans le secteur des communications électroniques, ce soit la personne physique dont les données sont traitées qui soit informée ou sollicitée (et en sus l'abonné pour ce qui concerne la Commission), s'il s'agit de personnes distinctes. Cette position s'imposerait au regard de la loi du 8 décembre 1992 qui s'articule autour de la notion de personne concernée, à savoir la personne physique dont les données font l'objet du traitement.

Dans les articles 122 et 123 analysés, nous constaterons que la loi ne traduit pas tout à fait cette exigence. En effet, d'une part, les dispositions utilisent les termes

1. L'utilisateur est défini par l'article 2, 12°, de la loi comme étant « une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public ».
2. L'utilisateur final est défini par l'article 2, 13°, de la loi comme étant « un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public »
3. C.P.V.P., avis n° 18/2007 relatif à la proposition de loi relative aux communications électroniques en vue d'assurer une meilleure protection de la vie privée pour les « services à données de localisation » ou les services de « géolocalisation » par téléphone portable, 27 avril 2007, pp. 2 et 3, www.privacycommission.be ; avis 2012/10 relatif au projet de loi portant des dispositions diverses en matière de communications électroniques, 21 mars 2012, p. 15, www.privacycommission.be.
4. Groupe de l'article 29, avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, *WP* 115, 25 novembre 2005, p. 7, http ://ec.europa.eu/justice/data-protection/.

« utilisateur final », qui peut être une personne physique ou une personne morale. Le concept mobilisé ne permet donc pas de viser spécifiquement la personne physique dont les données sont concernées. D'autre part, les dispositions concernées sont libellées sous une forme alternative (« l'abonné ou l'utilisateur », « l'abonné ou, le cas échéant, l'utilisateur ») de sorte qu'on peut difficilement en déduire une obligation d'informer, par exemple, l'un et l'autre. Il en résulte, à notre sens, une incertitude quant à la manière d'appliquer concrètement les dispositions dont question. Nous y reviendrons *infra* dans le cadre de l'analyse des articles 122, 123 et 129[1].

Ceci dit et pour être complet il convient encore de signaler qu'il pourrait y avoir des hypothèses où les deux lois ne s'appliquent pas cumulativement, en raison de différences, d'une part, quant aux personnes protégées par les dispositions de la loi du 13 juin 2005 et, d'autre part, quant aux critères d'application territoriale des deux lois.

En effet, il y a lieu de noter qu'en certaines dispositions, la loi du 13 juin 2005 va plus loin que la loi du 8 décembre 1992 puisqu'elle étend l'application de mécanismes de protection en matière de traitement de données à des personnes morales par le biais de la définition d'abonné et d'utilisateur, alors que la loi du 8 décembre 1992 ne prévoit que la protection des personnes physiques[2]. En effet, aux termes de l'article 2, 12° et 15° de la loi du 13 juin 2005, la loi entend, par « utilisateur », « une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public » et, par « abonné », « toute personne physique ou morale qui utilise un service de communications électroniques en exécution d'un contrat passé avec un opérateur ». Il est clair toutefois que l'opérateur ne sera tenu par les obligations découlant uniquement de la loi du 8 décembre 1992 qu'en ce qui concerne les abonnés personnes physiques. Ainsi, le droit d'accès ne sera octroyé en application de l'article 10 de la loi du 8 décembre 1992 que vis-à-vis des personnes physiques concernées et non des personnes morales.

Ensuite, si l'on s'en tient aux termes de la loi belge du 13 juin 2005 relative aux communications électroniques, il est envisageable qu'elle ait un champ d'application territorial qui n'est pas déterminé au regard des mêmes critères que ceux de la loi du 8 décembre 1992[3]. Il n'est donc théoriquement pas exclu que la loi du 13 juin 2005 trouve à s'appliquer alors que tel ne serait pas le cas de la loi du 8 décembre 1992.

Pour l'application de la loi du 8 décembre 1992, on se demandera si les traitements de données sont réalisés par un responsable de traitement dans le cadre d'un établissement sur le territoire belge[4]. Un établissement suppose l'exercice effectif et réel

1. Voy. chapitres 5.4 et 5.5.
2. Voy. la notion de donnée à caractère personnel qui vise « toute information concernant une personne physique identifiée ou identifiable » (art. 1er, § 1er, de la loi du 8 décembre 1992).
3. Cf. chapitre 5.2, section 2, *Infra*.
4. Article 3bis, 1°, de la loi du 8 décembre 1992.

d'une activité au moyen d'une installation stable, tandis que la forme juridique du responsable de traitement et l'existence d'une personnalité juridique ou non importent peu[1]. Pour déterminer si c'est la loi belge qui s'applique à un établissement (siège, filiale ou succursale), il convient donc de vérifier si c'est bien dans le cadre des activités de celui-ci que le traitement est effectué[2]. Si le responsable de traitement est établi hors du territoire de l'Union européenne, il est encore possible qu'il se voie appliquer la loi belge, dans l'hypothèse où il « [recourrait], à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge »[3]. Nous verrons sous le chapitre 5.2, section 2, que les critères utilisés pour déterminer le champ d'application territorial de la loi du 13 juin 2005 peuvent différer.

1. Voy., à cet égard, le considérant 19 de la directive (CE) n° 95/46 auquel se réfère l'exposé des motifs de la loi du 8 décembre 1992 (Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 27).
2. Th. Léonard voit également une autre condition implicite à l'application de la loi belge, à savoir que l'établissement dont question participe lui-même au traitement de données (Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *Guide juridique de l'entreprise*, titre XI, liv. 112.1, 2e éd., Bruxelles, Kluwer, 2004, p. 23).
3. Article 3, 2°, de la loi du 8 décembre 1992.

CHAPITRE 5.2. CHAMP D'APPLICATION MATÉRIEL, TERRITORIAL ET PERSONNEL DE LA LOI DU 13 JUIN 2005

1. Quelques notions clés de la loi pour appréhender le champ d'application matériel de la loi

Pour comprendre la portée des quelques dispositions que nous nous proposons d'analyser au sein de la loi du 13 juin 2005, il convient de saisir quelques notions clés de cette réglementation, parmi lesquelles celle d'opérateur qui est utile pour déterminer le champ d'application de certaines dispositions.

1.1. La notion d'opérateur

La loi du 13 juin 2005 entend principalement s'appliquer aux opérateurs fournisseurs de services de communication électroniques. Nous verrons toutefois, au point 2. Champ d'application territorial des dispositions qui s'adressent aux opérateurs, que certaines dispositions ont une portée plus large.

Pour déterminer qui est un opérateur au sens de la loi du 13 juin 2005, l'article 2, 11°, renvoie à l'article 9 de la loi qui spécifie qui sont les personnes qui doivent introduire une notification préalable. Autrement dit, l'opérateur est celui qui doit opérer une notification auprès de l'I.B.P.T[1]. préalablement au lancement de ses activités en application de l'article 9 de la loi. Cette disposition impose une obligation de notification préalable aux personnes qui fournissent ou revendent en leur nom propre et pour leur propre compte des services ou des réseaux de communications électroniques.

La notion d'opérateur intègre donc à la fois une dimension liée au type de services fournis et une autre inspirée par la réglementation des conditions pour prester de tels services en Belgique. L'approche du législateur belge est donc distincte de celle du

1. L'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (*cf.* art. 2, 1°, de la loi du 13 juin 2005).

législateur européen. En effet, les dispositions que nous analysons sont applicables au niveau européen au fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public (*cf.* art. 6 et 9 de la directive (CE) n° 2002/58). Ces deux concepts n'intègrent pas l'aspect réglementation de l'accès au marché, qui elle provient d'une autre directive du Paquet Télécom, la directive (CE) n° 2002/20 ou directive « Autorisation ».

Pour comprendre quelles sont les personnes concrètement visées, il nous faut revenir sur les notions évoquées dans cette disposition et sur ce que sont les « services de communications électroniques » et les « réseaux de communications électroniques ».

1.2. La notion de réseau de communications électroniques

Ces termes visent « les systèmes de transmission, et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de radiodiffusion et de télévision »[1].

La fourniture d'un réseau de communications électroniques est, quant à elle, définie comme étant « la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques »[2].

Autrement dit, on vise les entreprises qui fournissent l'infrastructure physique (les câbles) ou satellitaire qui permet la transmission des données.

Il convient également de noter d'emblée que la loi ne circonscrit pas la notion d'opérateur à des fournisseurs de réseaux *publics* de communications électroniques[3]. Les réseaux tout à fait privés[4] sont donc potentiellement concernés, même si des exceptions ont été apportées à l'obligation de notification, qui pourraient bénéficier aux fournisseurs de réseaux privés ou « non publics »[5].

---

1. Article 2, 3°, de la loi du 13 juin 2005.
2. Article 2, 4°, de la loi du 13 juin 2005.
3. Cette notion est toutefois définie à l'article 4, 10°, de la loi du 13 juin 2005, comme s'entendant d'« un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public permettant la transmission d'informations entre les points de terminaison du réseau ».
4. Il s'agirait, selon F. Dehousse et T. Zgajewski, d'un réseau dont l'accès n'est pas offert à tous. Les auteurs pointent qu'il pourrait s'agir, par exemple, d'un réseau interne d'une entreprise, ayant, le cas échéant, des sièges dans des localités différentes, ou d'une administration ou d'une borne Wi-Fi dans un hôtel (F. DEHOUSSE et T. ZGAJEWSKI, « Le nouveau régime des communications électroniques en Belgique à la suite de la loi du 13 juin 2005 », *J.T.*, 2006, p. 541).
5. Voy. les paragraphes 5 et 6 de l'article 9 commentés *infra* sous cette même section.

Comme le relève la doctrine, cela confère à la notion d'opérateur en droit belge une portée beaucoup plus vaste qu'en droit européen, dès lors que « la notion d'opérateur en droit européen est confinée aux fournisseurs de réseaux publics et n'est quant à elle pas étendue aux fournisseurs de réseaux privés ni aux fournisseurs de services »[1].

1.3. La notion de service de communications électroniques

Par ailleurs, par « service de communications électroniques », on entend « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, en ce compris les opérations de commutation et de routage, de signaux sur des réseaux de communications électroniques, à l'exception (a) des services consistant à fournir un contenu (à l'aide de réseaux et de services de communications électroniques) ou à exercer une responsabilité éditoriale sur ce contenu, à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et à l'exception (c) des services de la radiodiffusion y compris la télévision ».

Pour bien saisir cette notion, il convient d'en relever les différents éléments.

Un service *contre rémunération*

Seuls les services fournis « normalement contre rémunération » sont visés, c'est-à-dire non seulement les services payants, mais également ceux qui sont directement ou indirectement subventionnés par une activité économique. Ainsi, selon le Groupe de l'article 29[2], les services gratuits offerts par des fournisseurs d'accès entrent dans le champ d'application de la directive[3].

Un service *consistant entièrement ou principalement en la transmission de signaux sur des réseaux*

Les services de communications électroniques concernent donc des services de transmission. Il s'agit des services qui sous-tendent l'envoi physique de contenus,

---

1. Q. Coppieters 't Wallant, E. Lievens, R. Queck, D. Stevens et P. Valcke, « Le nouveau cadre réglementaire des communications électroniques : une avancée significative sur un terrain incertain ? », *R.D.T.I.*, 2006, p. 80.
2. Ce groupe, qui tient son nom du fait qu'il a été institué par l'article 29 de la directive (CE) n° 95/46, est un organe consultatif européen, composé entre autres de représentants de chaque autorité de contrôle des États membres et qui rend des avis.
3. Groupe de l'article 29, avis 7/2000 sur la proposition de la Commission européenne d'une directive du Parlement européen et du Conseil concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 – *COM*(2000) 385, 2 novembre 2000, *WP* 36, p. 5, http://ec.europa.eu/justice/data-protection/.

c'est-à-dire l'exploitation d'un réseau et la transmission même des contenants sur ce réseau[1]. Sont donc considérés comme tels les fournisseurs d'accès à Internet dans la mesure où le service vise précisément à assurer la transmission de données à leurs clients par le biais d'Internet. En revanche, le fournisseur d'un service de *Cloud Computing*, par exemple, ne sera pas considéré comme un fournisseur de services de communications électroniques lorsque le fournisseur n'assure pas lui-même le transport des données vers les lieux de stockage des données.

De par la définition de la loi sont exclus les services consistant à fournir un contenu ainsi que des services de la société de l'information (tels que définis à l'art. 2 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information) qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

Ceci étant, il y a lieu de souligner que les critères d'application sont de nature fonctionnelle, et non de nature organique. Afin de déterminer si la loi s'applique ou non, il y a lieu de tenir compte des types de services qu'un fournisseur livre effectivement[2]. Le Groupe de l'article 29 cite, à cet égard, dans le cadre d'une réflexion sur cette notion par rapport à la directive-cadre du Paquet Télécom qui contient une définition similaire[3], l'exemple d'un fournisseur de service Internet qui fournit également un contenu, en hébergeant son propre site portail : le fournisseur de service Internet est amené à appliquer la directive (CE) n° 95/46 à l'ensemble de ses activités (service de la société de l'information) et la directive (CE) n° 2002/58 aux activités dans lesquelles il joue le rôle de fournisseur d'accès (service de communications électroniques)[4].

Pour ce qui est du service de messagerie tel que ceux offerts par Yahoo ou Gmail, la question n'est pas simple. En effet, dans ce type de service le prestataire de services n'assure pas le transport des informations sur le Web, mais se limite *a priori* à fournir une application de messagerie électronique qui, elle, fonctionne grâce à l'Internet. On serait tenté de considérer qu'il ne s'agit pas d'un service de communication électronique[5]. Toutefois, le considérant 10 de la directive-cadre (CE) n° 2002/21 sème le

1. J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (anciennement revue* Ubiquité*)*, 2003, pp. 13 et s.
2. Pour des développements plus complets sur cette notion dans le cadre des définitions de la directive (CE) n° 2002/58, voy. J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (anciennement revue* Ubiquité*)*, 2003, pp. 13 et s.
3. Elle définit le service de communications électroniques comme étant « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive (CE) n° 98/34 qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques » (art. 2, 6°, de la directive (CE) n° 2002/21 du Parlement et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques).
4. Groupe de l'article 29, avis 7/2000 sur la proposition de la Commission européenne d'une directive du Parlement européen et du Conseil concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 – *COM*(2000) 385, *WP* 36, 2 novembre 2000, p. 5, http ://ec.europa.eu/justice/data-protection/.
5. Voy., à cet égard, N. Vandezande, « Yahoo ! als operator of verstrekker », *A&M*, 2011, p. 222.

doute en ce qu'il considère à propos des services fournis en ligne que les services de téléphonie vocale[1] et de transmission de courriers électroniques sont couverts par la directive et, donc, inclus dans le champ des services de communications électroniques.

Il est vrai que, si on privilégie une approche fonctionnelle, on doit constater que ce type de service permet l'acheminement de communications électroniques entre un nombre fini de personnes, nonobstant le fait que le système sous-jacent à ces communications n'est pas tout à fait identique aux communications via des serveurs de courriers électroniques. Dans un arrêt du 18 janvier 2011, la Cour de cassation s'est prononcée sur la qualification de Yahoo ! Inc. comme fournisseur de service de communication électronique dans le cadre de l'application de l'article 46*bis* du Code d'instruction criminelle et a considéré que la personne qui fournit un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques[2].

La question semble désormais tranchée par le législateur. Lors de l'élaboration de la loi du 30 juillet 2013[3], il a été précisé le service de messagerie électronique par l'internet n'entre pas dans le champ d'application de la définition du service de communications électroniques au sens de l'article 2, 5° de la loi du 13 juin 2005 car ce service ne consiste pas à transmettre des signaux mais à fournir, à l'aide de réseaux et services de communications électroniques, du contenu transmis[4]. Nous verrons toutefois que le législateur a étendu l'obligation de conservation de données et de collaboration avec les autorités judiciaires à ces prestataires de services. Nous y reviendrons dans le Chapitre 5.4, section 4.7. La collaboration avec certaines autorités., *infra.*

Caractère électronique de la communication

La notion de « communications électroniques » remplace le concept de « télécommunications » de la directive (CE) n° 97/66.

La notion de « communications électroniques » fait allusion à toute communication ou transmission de signaux indépendamment du médium utilisé et comprenant l'acheminement « par câble, par voie hertzienne, par moyen optique ou par d'autres

1. On pourrait penser aux services de téléphonie via Internet (le *Voice over IP*). La qualification de service de VoIP comme service de communication électronique a toutefois évolué et est abordée de manière plus nuancée suivant les caractéristiques du service fourni dans différents documents de travail de la Commission (voy., sur ce point, R. ROBERT, « *Voice over IP* : une réglementation sur la bonne voie ? », *R.D.T.I.*, 2008, pp. 431 et s.).
2. Cass., 18 janvier 2011, R.G. n° P.10.1347.N/4.
3. Il s'agit de la loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, entrée en vigueur le 2 septembre 2013.
4. Projet de loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *Doc. parl.*, Chambre, Législature n°53, n° 2921/001, p. 12.

moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec communication de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câbles de télévision, quel que soit le type d'information transmise »[1].

Nous reviendrons sur cette notion dans le chapitre 5.3, section 2.2.1. Communications électroniques., lorsque nous analyserons la portée du secret des communications électroniques.

Un service de transmission *point à point*

Par ailleurs, il nous apparaît que la loi ne vise que le traitement des données mis en œuvre dans le cadre des services d'acheminement d'informations point à point, dès lors qu'elle exclut les services de radiodiffusion sonore et télévisuelle[2]. On pense concrètement à la téléphonie fixe et mobile et aux services d'Internet et aux courriers électroniques.

En ce sens, si l'on a égard à la directive (CE) n° 2002/58, sont exclues du champ d'application de la directive « les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit »[3].

1.4. Les personnes qui échappent à la qualification d'opérateur

Il existe toutefois des personnes qui ne seront pas qualifiées d'opérateurs : les paragraphes 5 et 6 de l'article 9 de la loi du 13 juin 2005 précisent que la notification visée par cette disposition ne sera pas requise :

- en cas de fourniture ou de revente de réseaux ou services de communications électroniques *qui ne traversent pas le domaine public.*
  Cette hypothèse concerne, par exemple, des réseaux qui se trouvent exclusivement sur un domaine privé, tel un LAN[4] au sein d'une entreprise, et qui ne pas-

1. Article 1er, (a), de la directive (CE) n° 2002/21.
2. À noter qu'en droit belge, cette exclusion recouvre également une autre réalité : celle de la répartition de compétences faisant que la réglementation en matière de radiodiffusion sonore et télévisuelle échappe pour une grande part à la compétence du législateur fédéral (voy., à ce sujet, J. Jost et R. Queck, « Communications électroniques et répartition des compétences : chantiers importants en cours », *R.D.T.I.*, 2009, pp. 5 à 27).
3. Article 2, (d), de la directive 2002/58.
4. « Local Area Network » ou « réseau local » qui correspond à un réseau informatique.

sent pas sur le domaine public (ne serait-ce que pour faire le lien avec un réseau dans un autre bâtiment)[1] ;

- pour la fourniture ou la revente de services ou réseaux de communications électroniques exclusivement destinés à une personne morale, dans laquelle le fournisseur ou le revendeur possède une participation majoritaire, ou destinés à des personnes physiques ou des personnes morales dans le cadre d'une convention dans laquelle des services ou réseaux de communications électroniques sont mis à disposition accessoirement et uniquement à titre d'assistance. On peut penser, par exemple, à un service de cryptographie qui impliquerait un détournement du trafic pour crypter avant que la transmission des informations ne se poursuive sur les réseaux de communications. Dans ce cas, le service principal est un service de cryptage même si, accessoirement, il y a une partie de la transmission des informations qui est assurée par le prestataire de services.

Les personnes qui sont visées aux paragraphes 5 et 6 ne seront donc pas considérées comme des opérateurs au sens de la loi[2].

Ces exclusions ont été introduites postérieurement à l'adoption de la loi du 13 juin 2005[3] pour corriger la portée potentiellement extrêmement large de la notion d'opérateur. La doctrine avait pointé à propos du texte initial : « [...] si l'on prend le champ de cette obligation à la lettre, il donne à l'extrême un résultat pour le moins étonnant : un particulier mettant ses trois ordinateurs en réseau chez lui pourrait être considéré comme fournisseur de réseau de communications électroniques et serait dès lors soumis à l'obligation de notification. En l'état, le texte vise en effet également les réseaux privés et ce, sans distinction »[4].

1. La mise en place d'un réseau privé qui traverserait le domaine public devrait donc donner lieu à notification. Sur ce point, le champ d'application de la législation belge se distingue également de celui décrit dans la directive (CE) n° 2002/58 qui vise, quant à lui, la fourniture d'un réseau public de communications ou d'un service de communications électroniques accessibles au public (*cf.* art. 6 et 9 de la directive (CE) n° 2002/58.) et exclut de son champ d'application les réseaux privés (concernant ce point, voy. H. Lutz et C. Henckel, « Data protection and privacy », *In Law and Regulation of Electronic Communication In Europe*, 6e éd., Frankfort, 2013, p. 123 ; J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (anciennement revue* Ubiquité*)*, 2003, p. 18).
2. Il demeure toutefois que ces catégories de fournisseurs sont susceptibles d'être soumises à des obligations similaires à celles des opérateurs en matière de rétention de données et de collaboration avec les autorités judiciaires et comme le prévoit le paragraphe 7 de l'article 9. À ce jour, l'arrêté royal qui doit organiser les modalités de cette obligation de rétention de données n'a pas encore été adopté.
3. Par l'article 92 de la loi du 20 juillet 2006 portant des dispositions diverses.
4. Q. Coppeters 't Wallant, E. Lievens, R. Queck, D. Stevens et P. Valcke, « Le nouveau cadre réglementaire des communications électroniques : une avancée significative sur un terrain incertain ? », *R.D.T.I.*, 2006, p. 79. Ces auteurs avançaient toutefois plusieurs arguments tendant à limiter la portée de cette disposition (*ibid.*).

2. Champ d'application territorial des dispositions qui s'adressent aux opérateurs

2.1. Le caractère hybride de la loi

La loi du 13 juin 2005 présente un caractère hybride. En effet, bien qu'elle tende principalement à réglementer la fourniture de réseaux et de services de communications en Belgique, elle contient certaines dispositions qui vont s'appliquer à tout un chacun. On retrouve cette dualité de dispositions dans la section de la loi analysée dans le cadre de cette contribution et intitulée « Secret des communications, traitement des données et protection de la vie privée ». Il en résulte, à notre sens, de possibles différences en ce qui concerne le champ d'application territorial et personnel de la loi selon les dispositions concernées.

2.2. Champ d'application des dispositions qui s'adressent aux opérateurs

La loi du 13 juin 2005 ne contient pas de disposition spécifique déterminant son champ d'application territorial.

L'effet de la loi sur le plan territorial nous paraît être également fonction de la notion d'opérateur. La loi vise en grande partie à réglementer les droits et obligations des opérateurs. Ainsi en est-il par exemple des articles 122 et 123 de la loi que nous analyserons au chapitre 5.4. Pour savoir si une personne est tenue ou non au respect de ces dispositions, il faut déterminer si elle a ou non la qualité d'opérateur.

Pour ce qui concerne les entreprises localisées hors du territoire belge, il est prévu qu'elles ne doivent notifier en Belgique que si elles entendent fournir des réseaux ou des services de communications électroniques en Belgique[1]. La doctrine relève à cet égard que la notification n'est pas nécessaire s'il s'agit simplement pour l'entreprise active sur un territoire frontalier de demander l'accès et l'interconnexion[2]. Il suffit, dans ce cas, qu'elle soit un opérateur au sens de la réglementation de son pays d'origine[3].

Il résulte de ce qui précède que la notion d'opérateur est étroitement liée à la fourniture de réseaux ou de services de communications *en Belgique*.

---

1. Article 10, alinéa 2, de la loi du 13 juin 2005.
2. O. Coppieters 't Wallant, E. Lievens, R. Queck, D. Stevens et P. Valcke, « Le nouveau cadre réglementaire des communications électroniques : une avancée significative sur un terrain incertain ? », *R.D.T.I.*, 2006, p. 79.
3. Article 10, alinéas 2 et 3, de la loi du 13 juin 2005.

3. Champ d'application des dispositions qui ne s'adressent pas aux seuls opérateurs

Certaines dispositions ne s'appliquent pas uniquement aux opérateurs. Tel est le cas des articles 124 – concernant le secret des communications électroniques – et 129 – qui réglemente l'utilisation des *cookies* et autres logiciels espions. Ces dispositions s'appliquent à quiconque tend à poser certains actes prohibés ou soumis à conditions par les dispositions concernées. Il n'est, à cet égard, pas fourni de critère d'application territoriale de ces dispositions.

Pour ce qui concerne l'article 129, l'on pourrait toutefois avoir égard aux personnes que cette disposition entend protéger. En effet, cette disposition identifiait, dès sa version initiale au moment de l'adoption de la loi du 13 juin 2005, comme bénéficiaires de la protection octroyée par cette disposition les « abonnés » (et depuis une loi du 10 juillet 2012[1] également, les « utilisateurs »).

Au sens de l'article 2, 15°, l'abonné est « toute personne physique ou morale qui utilise un service de communications électroniques en exécution d'un contrat passé avec un opérateur et qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public ». Eu égard au fait que la notion d'opérateur renvoie à la fourniture de services sur le territoire belge, il nous paraît raisonnable d'en inférer que l'article 129 tend à s'appliquer aux abonnés d'un service de communications fourni sur le territoire belge.

L'ajout d'une référence à l'utilisateur final[2] a pour but d'étendre la protection aux personnes qui font effectivement usage des services et qui ne sont pas toujours les abonnés (tel est le cas, p. ex., dans le cadre des relations de travail : l'abonné est bien souvent l'employeur, tandis que les utilisateurs finals sont les travailleurs). Il ne remet pas en cause le rattachement qui nous semble devoir être fait avec le lieu de fourniture des services, à savoir le territoire belge.

L'article 124 ne contient pas non plus de rattachement direct au territoire belge. Il se réfère à la prise de connaissance d'informations transmises par voie de communications électroniques ou de données en matière de communications électroniques. La notion de « communications électroniques » n'est elle-même pas liée au territoire belge. Comme exposé précédemment, ce n'est qu'un détour par la notion d'opérateur qui permet de faire le lien avec le territoire belge. Or, en l'espèce, la disposition

1. *Cf.* article 90 de la loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques.
2. Qui est, quant à lui, défini par l'article 2, 13°, de la loi comme étant une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public et qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public.

s'impose non seulement aux opérateurs, mais également à toute personne en général, sans lien avec le territoire.

Il n'y a donc pas d'élément explicite pour définir le critère de rattachement au territoire belge, mais on pourrait avoir égard au fait que la loi belge a principalement pour vocation de réglementer le secteur des communications électroniques en Belgique pour considérer qu'un lien avec un service de communications électroniques fourni en Belgique soit requis.

Par ailleurs, compte tenu du fait que le non-respect de l'article 124 est sanctionné pénalement à l'article 145 de la loi du 13 juin 2005, on pourrait, en cas d'élément d'extranéité, appliquer la théorie de l'ubiquité développée en jurisprudence et en doctrine lorsqu'il s'agit de déterminer l'application dans l'espace d'une infraction pénale[1].

Selon cette théorie, lorsque des éléments constitutifs de l'infraction ont été commis sur plusieurs territoires nationaux, il suffit qu'un de ces éléments constitutifs ait eu lieu en Belgique pour que l'infraction soit réputée commise en Belgique et, donc, que les juridictions belges soient compétentes pour en connaître[2]. Il suffit qu'un élément matériel – non purement intentionnel – constitutif de l'infraction ait été réalisé sur le territoire du Royaume. En revanche, il n'est pas requis que l'infraction ait été entièrement commise en Belgique ou qu'elle y ait été consommée, dans l'hypothèse d'une infraction instantanée impliquant la réalisation d'un résultat[3].

É. Marique relève, en matière d'infraction commise par le biais d'Internet, que la théorie de l'ubiquité permet au juge belge de connaître des infractions quand l'auteur opère en Belgique ou lorsque le système (serveur) informatique se trouve en Belgique ou, encore, lorsque le dommage se réalise en Belgique[4]. L. Kerzmann rappelle encore à ce sujet qu'en matière informatique, la juridiction du lieu où l'acte délictueux a été constaté est compétente en vertu de cette théorie de l'ubiquité[5].

Nous n'avons pas connaissance de cas de jurisprudence dans lesquels l'application territoriale de cette disposition ait été analysée. Il résulte toutefois de ce qui précède que l'application de l'article 124 devrait, nous semble-t-il, requérir que les actes interdits, telle la prise de connaissance des informations transmises, interviennent grâce à l'utilisation d'un service de communication fourni en Belgique (un abonné ou un utilisateur d'un service de communication électronique fourni en Belgique) ou concer-

1. Voy., sur cette théorie, F. Kuty, *Principes généraux d'application de la loi pénale*, t. I, Bruxelles, Larcier, 2007, pp. 314 et s.
2. Voy., notamment, Cass., 24 janvier 2001, *Pas.*, 2001, p. 168 ; Cass., 14 novembre 2000, *Pas.*, 2000, p. 1746.
3. L. Kerzmann, « L'affaire Yahoo ! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle ? », *R.D.T.I.*, 2011, p. 122.
4. É. Marique, « Les jeux de hasard au moyen des instruments de la société de l'information », *Rev. dr. pén.*, 5/2009, p. 430.
5. L. Kerzmann, « L'affaire Yahoo ! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle ? », *R.D.T.I.*, 2011, p. 122.

nent une information ou des données de communications transmises par le biais d'un service de communications électroniques fourni en Belgique.

Une autre option serait d'appliquer systématiquement les critères de la loi du 8 décembre 1992 dès qu'il est question de traitement de données. Cette solution peut s'imposer au regard du rapport entre les directives (CE) n^{os} 2002/58 et 95/46, puisqu'au niveau du cadre européen, il est précisé que les dispositions de la première directive entendent régir des traitements de données à caractère personnel dans le cadre du secteur des communications électroniques[1]. En ce sens, nous relevons que, dans un avis du 27 février 2013, le Groupe de l'article 29 semble préconiser l'application des critères d'application territoriale de la directive (CE) n° 95/46 pour l'application de l'article 5, § 3, de la directive (CE) n° 2002/58 qui est transposé à l'article 129[2]. On se demandera, pour l'application de la loi du 8 décembre 1992[3], où est établi le responsable de traitement. La loi belge du 8 décembre 1992 s'appliquera si le traitement est mis en œuvre dans le cadre d'un établissement du responsable du traitement sur le territoire belge[4] ou, éventuellement, si le responsable de traitement est établi hors du territoire de l'Union européenne, s'il recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge[5].

1. Voy. Chapitre 5.1., section 3.1., *supra*.
2. Groupe de l'article 129, « Opinion 02/2013 on apps on smart devices », 27 février 2013, *WP* 202, p. 7, http ://ec.europa.eu/justice/data-protection/.
3. *Cf.* Chapitre 5.1., *supra*.
4. Article 3*bis*, 1°, de la loi du 8 décembre 1992.
5. Pour une réflexion sur l'application de ces derniers critères aux *cookies* visés par l'article 129 de la loi du 13 juin 2005, voy. Groupe de l'article 29, Document de travail sur l'application internationale du droit de l'Union européenne en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites Web établis en dehors de l'Union européenne, 30 mai 2002, *WP* 56, p. 11, http ://ec.europa.eu/justice/data-protection/.

CHAPITRE 5.3.
LE SECRET DES COMMUNICATIONS ÉLECTRONIQUES[1]

1. Quelques propos introductifs sur le cadre légal

La loi du 13 juin 2005 transpose notamment l'article 5, §§ 1er et 2, de la directive (CE) n° 2002/58.

Le principe du secret des communications y est défini à l'article 124 et les exceptions aux articles 125 et 128 de la loi. Les articles 124 et 125 remplacent les articles 109*ter*D et 109*ter*E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (loi Télécom) qui ont été abrogés par la loi du 13 juin 2005 relative aux communications électroniques.

En sus de cette loi subsistent les articles 314*bis* et 259*bis* du Code pénal qui prohibent également certains actes de prise de connaissance des communications électroniques[2].

À ce propos, il convient de souligner que la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées[3] avait modifié la portée des dispositions contenues dans la loi du 21 mars 1991 pour qu'elles ne portent plus sur le contenu des communications, mais sur les données de communications. À partir de 1994, on a donc vu s'affirmer, en doctrine et en jurisprudence, une distinction entre la

---

1. Cette section s'inspire largement, tout en l'actualisant et en y incluant des développements nouveaux, d'une partie de la contribution suivante : R. Robert et K. Roser, « Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu du travail », *in Le droit du travail à l'ère du numérique*, Limal, Anthemis, 2011, pp. 252 à 275. Pour une étude plus spécifique du cas du secret des communications électroniques dans le cadre des relations de travail, nous renvoyons à cette contribution.
2. L'article 314*bis* prévoit notamment que :
   « § 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque :
   1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications ;
   2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque [...]. »
   L'article 259*bis* a un objet similaire si ce n'est que l'interdiction s'adresse aux officiers, fonctionnaires publics, dépositaires ou agents de la force publique qui poseraient de tels actes à l'occasion de l'exercice de leurs fonctions.
3. *M.B.*, 25 janvier 1995, p. 01542.

réglementation de la protection du contenu des communications, d'une part, et celle des données de communications, d'autre part. Le contenu était protégé par les articles 314*bis* et 259*bis* du Code pénal, tandis que les données de communications l'étaient par la loi du 21 mars 1991[1].

Nous verrons que le libellé ambigu de l'article 124 de la loi du 30 juin 2005 met à mal cette distinction et qu'à présent, le contenu des communications est régi à la fois par les dispositions précitées du Code pénal et par l'article 124.

2. Portée du secret des communications

2.1. Texte légal

L'article 124 de la loi du 13 juin 2005 relative aux communications électroniques (et qui remplace l'article 109*ter*D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [loi Télécom]) prévoit :

> « S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :
>
> 1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ;
>
> 2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ;
>
> 3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ;
>
> 4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non. »

1. F. Hendrickx, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, p. 188.

2.2. Communications visées

2.2.1. Communications électroniques

L'article 124 vise les communications électroniques. Si l'on en revient à la notion de « communications électroniques », on ne peut manquer de constater qu'elle est extrêmement large.

La loi du 13 juin 2005 ne contient pas de définition spécifique de la notion de « communications électroniques », mais l'article 2, 5°, de la loi y fait indirectement référence dans la définition donnée à un service de communications électroniques[1]. Dans la loi du 13 juin 2005, la réglementation des services de communications électroniques est affranchie de toute référence à des services fournis sur un *réseau public*. De ce fait, des transmissions de données transitant sur un réseau privé, par exemple un réseau privé d'une entreprise, peuvent parfaitement faire l'objet de la protection.

La directive-cadre du Paquet Télécom donne une définition plus complète de cette notion de communication électronique comme étant « toute transmission de tous types de signaux (voix, images, etc.) autres que ceux de la radiodiffusion ou de la télévision, indépendamment du médium utilisé et comprenant l'acheminement par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec communication de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câbles de télévision[2] ».

Elle englobe donc les communications téléphoniques, les courriels, SMS, MMS, télex et connexion à l'Internet[3]. Il nous semble que cela peut également concerner les connexions à un réseau ou à un système informatique.

En ce sens, la Commission de la protection de la vie privée[4] a considéré, dans un avis 18/2005, qu'« en ce qui concerne la collecte de données de communication, et

1. Pour rappel, il s'agit de la « transmission de signaux sur des réseaux de communications électroniques, à l'exception (a) des services consistant à fournir un contenu (à l'aide de réseaux et de services de communications électroniques) ou à exercer une responsabilité éditoriale sur ce contenu, à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et à l'exception (c) des services de la radiodiffusion y compris la télévision ».
2. Article 1er, (a), de la directive (CE) n° 2002/21 du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (« directive- cadre »).
3. P. DEGOUS et S. VAN WASSENHOVE, *Nouvelles technologies et leur impact sur le droit du travail*, Courtrai/Bruxelles, UGA, 2010, p. 37.
4. Il a été instauré, dans chaque État de l'Union européenne, une autorité de contrôle chargée de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la directive (CE) n° 95/46. En Belgique, il s'agit de la Commission de la protection de la vie privée qui émet des avis et des recommandations sur des problématiques particulières posées par l'application de la loi du 8 décembre 1992 et, plus largement, à toute la législation relative à la protection des données à caractère personnel.

notamment d'éventuels loggings, la Commission rappelle par ailleurs que le principe de confidentialité des données de télécommunication s'applique sans préjudice de la nécessaire adoption de mesures de sécurité techniques et organisationnelles telles que prévues à l'article 16 de la loi, destinées à sécuriser l'accès aux réseaux et à assurer de façon globale la protection des données à caractère personnel. L'enregistrement de loggings dans cette perspective est admissible et même souhaitable, mais il doit être effectué dans une perspective de protection des données, sans détournement de finalité et réutilisation à des fins de contrôle permanent des employés »[1].

En revanche, le fait de publier des informations sur une page Internet (p. ex., du type blog) n'entraîne pas la protection du secret des communications quant au contenu de la page. Seules les données relatives aux connexions des internautes à la page concernée sont protégées.

Ainsi en est-il également, nous semble-t-il, de l'utilisation de certains outils mis à la disposition des utilisateurs du service de réseautage social pour communiquer avec d'autres membres et qui permettent d'« éditer » des messages sur une page Web (tel le « mur » de Facebook). Ces échanges d'informations ou de communications ne sont, selon nous, pas protégés par le secret des communications électroniques. Il s'agit d'informations qui ne sont, du reste, pas destinées à un nombre fini de parties, mais simplement auxquelles il est donné accès, le nombre de personnes pouvant y accéder étant susceptible de varier selon les paramètres du profil et l'évolution du nombre de personnes cooptées par le titulaire du profil comme « amis »[2].

2.2.2. Communications privées

La protection du secret des communications s'articule de longue date autour des notions de communications privées et de communications publiques[3]. La communication publique est celle destinée à tous, tandis que la communication privée n'est destinée qu'à un certain nombre de personnes[4].

---

1. C.P.V.P., avis 18/2005 relatif à un projet d'arrêté du Gouvernement de la Communauté française relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII, 9 novembre 2005, pp. 3 et 4, www.privacycommission.be.
2. K. Rosier et S. Gilson, « La vie privée du travailleur face aux nouvelles technologies de communication et à l'influence des réseaux sociaux. L'employeur est-il l'ami du travailleur sur Facebook ? », *in* K. Rosier (dir.), *Le droit du travail à l'ère numérique. Les technologies de l'information et de la communication dans les relations du travail*, Limal, Anthemis, 2011, pp. 410 et 411.
3. Cette distinction est envisagée dans les travaux préparatoires relatifs à l'article 314*bis* qui participe également à la protection du secret des communications (projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. parl.*, Sénat, 1992-1993, n° 843/1, p. 7).
4. O. Ruckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, p. 44.

Ainsi, tous les courriels ou SMS échangés dans un contexte du travail revêtiront un caractère privé[1].

Certains auteurs ou décisions de jurisprudence[2], lorsqu'ils indiquent que l'employeur ne peut consulter des courriels reçus ou envoyés par le travailleur, se plaisent à souligner que la protection ne vaut que lorsque la communication revêt un caractère privé. Ils ont laissé entendre qu'une telle ingérence aurait, par contre, été admissible si les courriels avaient été de nature strictement professionnelle[3].

Nous relevons à titre d'illustration les décisions suivantes.

- Dans un jugement du 19 mars 2008, le Tribunal du travail de Liège indique que « le caractère mixte d'un échange de correspondance lui enlève son caractère professionnel, de sorte que les principes constitutionnels du secret des lettres et du respect de la vie privée doivent s'appliquer dans toute leur rigueur »[4].
- Dans un arrêt du 26 avril 2010, la Cour du travail de Liège considère que deux travailleurs ont pu valablement marquer leur accord sur un système de contrôle décrit dans un avenant au contrat de travail et prévoyant que tous les courriels reçus ou adressés via l'adresse de courrier électronique professionnelle des travailleurs peuvent être consultés sans l'autorisation préalable et que le mot de passe de la messagerie professionnelle sera considéré comme personnel, mais non confidentiel[5]. Dans son appréciation, la Cour tient compte du fait que les travailleurs pouvaient bénéficier d'une adresse privée constituée par l'employeur dont ils pouvaient faire un usage raisonnable pendant les heures de travail. Elle souligne au passage qu'il appartient à l'employé de veiller à ce que seuls des courriels professionnels se trouvent dans la boîte professionnelle. Ce faisant, elle estime que l'employeur pouvait prendre connaissance de tous les courriels de la boîte professionnelle sans le consentement de toutes les parties à la communication, s'éloignant ainsi de l'interprétation donnée à la portée de l'article 124 précité.
- Le Tribunal du travail de Nivelles, dans un jugement du 31 mai 2011, estime que, lorsque l'adresse attribuée à une travailleuse est de type impersonnel (secretariat@nomdesociété), qu'il n'y a pas de mot de passe protégeant l'accès à la boîte de courriers électroniques, que cette adresse est utilisée par des tiers pour envoyer des courriers au chef de l'entreprise, il n'y a pas lieu de considérer que

1. J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 84 ; P. Degous et S. Van Wassenhove, *Nouvelles technologies et leur impact sur le droit du travail*, Courtrai/Bruxelles, UGA, 2010, p. 38.
2. C. trav. Liège (9e ch.), 26 avril 2010, R.G. n° 2009/AL/36.389, www.cass.be ; Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. n° 360.454, www.cass.be ; C. trav. Liège, 20 mars 2006, *R.R.D.*, 2006, pp. 89 à 101, note K. Rosier et S. Gilson ; Trib. trav. Malines, 22 octobre 2002, *Chron. D.S.*, 2003, pp. 201 à 203.
3. F. Lagasse, « La vie privée et le droit du travail », *Chron. D.S.*, 1997, p. 424. ; C. trav. Bruxelles (4e ch.), 3 mai 2006, R.G. n° 45.922, www.cass.be.
4. Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. n° 360.454, www.cass.be.
5. C. trav. Liège (9e ch.), 26 avril 2010, R.G. n° 2009/AL/36.389, www.cass.be.

les courriels adressés à la travailleuse sur cette adresse sont des communications « privées » protégées par l'article 124 de la loi du 13 juin 2005[1]. Le tribunal se fonde sur l'idée que la boîte de courriers électroniques était techniquement accessible à d'autres personnes que la secrétaire pour considérer que les communications qui s'y trouvent ne sont pas privées, indépendamment de la question de savoir si ces communications étaient ou non destinées à tout un chacun.

Ces raisonnements relevés en jurisprudence nous paraissent méconnaître la portée de l'article 124, dès lors que la loi n'opère nullement une telle distinction.

Ceci dit, on notera que la C.C.T. n° 81[2] contient une affirmation dans le préambule aux termes de laquelle, « lorsque l'objet et le contenu des données de communications électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter sans autre procédure » et l'article 11, alinéa 3, qui la reproduit au sein de la Convention. Le glissement d'une distinction communication privée/publique, vers une distinction communication privée/professionnelle a été introduit par cette C.C.T. Il convient toutefois de relever que, dans un arrêt du 15 décembre 2004, la Cour du travail d'Anvers a constaté que cette dernière distinction est contraire à l'article 8 CEDH ainsi qu'aux articles 314*bis* du Code pénal et 109*ter*D de la loi du 21 mars 1991[3], et à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[4].

2.3. Les informations protégées

Les actes prohibés visent à garantir la confidentialité de certaines informations que l'on peut diviser en trois catégories.

2.3.1. L'identité des personnes concernées

L'article 124, en son alinéa 2, vise expressément l'identité des personnes concernées tant par la transmission que par son contenu. Ceci implique qu'est interdite la consultation des données relatives à l'identité de l'expéditeur et du ou des destinataires des messages. La référence au contenu implique, si l'on veut donner une portée utile à cette précision, que les personnes qui sont concernées par le contenu (p. ex., citées dans le courrier électronique) sont, elles aussi, visées.

---

1. Trib. trav. Nivelles (sect. Wavre, 2e ch.), 31 mai 2011, inédit, R.G. n° 09/1536.
2. Convention collective de travail relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau, adoptée le 26 avril 2002 et qui a été rendue obligatoire par arrêté royal du 12 juin 2002, *M.B.*, 26 janvier 2002, p. 29489.
3. Encore en vigueur au moment de l'adoption de la C.C.T. n° 81.
4. C. trav. Anvers (sect. Anvers), 15 décembre 2004, *Chron. D.S.*, 2006, p. 146.

2.3.2. Les données de communications électroniques

L'alinéa 3 de l'article 124 a trait aux données de communications électroniques, en ce compris les données de trafic et les données de localisation définies aux articles 122 et 123 de la loi du 13 juin 2005.

Par « données de communications électroniques », on entend les données relatives aux communications électroniques qui transitent par réseau telles que l'adresse de courrier électronique de l'expéditeur et du destinataire, l'heure de l'envoi et de la réception, les données de routage, la taille du message, la présence de pièces jointes, etc.[1].

Le constat opéré à l'époque où l'article 109*ter*D de la loi Télécom était encore en vigueur selon lequel l'interdiction de la prise de connaissance des données de communications constituait un obstacle majeur à la prise de connaissance du contenu reste donc d'application.

En effet, la prise de connaissance du contenu d'une communication entraînera souvent la prise de connaissance des données de communications (adresse électronique de l'expéditeur et du destinataire, date et heure de la communication...) si bien que l'interdiction – non limitée à la durée de la transmission – de la prise de connaissance des données de communications constituera alors un obstacle à la prise de connaissance du contenu de la communication.

2.3.3. L'information transmise ou la transmission de l'information ?

L'article 124, 1°, de la loi du 13 juin 2005 vise la prise de connaissance de « l'existence » d'une information de toute nature transmise par voie de communication électronique.

C. de Terwangne, J. Herveg et J.-M. Van Gyseghem relèvent, à propos de cet alinéa 1er, qu'« [i]l semble, de prime abord, ne viser que les données liées au transport des communications et non le contenu de celles-ci »[2]. L'interprétation de l'alinéa premier de l'article 124 précité nous paraît effectivement des plus malaisées. Le libellé vise « la prise de connaissance de l'existence d'une information », et non de l'information elle-même, ce qui aurait permis d'en déduire que le contenu de la disposition était assurément visé. Les travaux préparatoires n'apportent aucune précision à cet égard.

---

1. O. Ruckaert, « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 210 ; pour une application, voy. C. trav. Bruxelles, 10 février 2004, R.G. 44002, www.cass.be. À propos des articles qui ont précédé l'article 124 (à savoir l'art. 111, 3°, devenu l'art. 109*ter*D, 3°, de la loi du 21 mars 1991), F. Hendrickx estimait toutefois que la protection ne concernait pas en tant que telle toutes les données qui sont généralement connues, comme le nom, l'adresse, etc., de l'utilisateur (F. Hendrickx, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, p. 188).
2. C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication*, Bruxelles, Kluwer, 2005, p. 46.

Pourtant, l'enregistrement de ces données nous semble se confondre avec les actes visés à l'alinéa 3 de l'article 124 (données de communications électroniques). On peut dès lors se demander quelle est l'utilité d'une telle disposition si ce n'est de viser plutôt que le transport, la communication elle-même – en ce compris son contenu.

À notre connaissance, la question n'a pas été abordée en tant que telle par les juridictions du fond qui semblent considérer pour acquis que l'article 124 fait obstacle à la prise de connaissance du contenu des communications sans s'étendre sur le sujet.

Un arrêt de la Cour de cassation du 1er octobre 2009[1] nous semble valider cette position. Dans cet arrêt, la Cour énonce :

« En vertu de l'article 124, 1° et 4°, de la loi du 13 juin 2005 relative aux communications électroniques, s'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement, ni faire un usage quelconque de l'information obtenue intentionnellement ou non.

Cet article exclut dès lors notamment la prise de connaissance intentionnelle de l'existence d'un courriel, ainsi que l'usage de cette connaissance ou de l'information qui est ainsi obtenue intentionnellement ou non, par quiconque n'y a pas été autorisé au préalable.

Quiconque prend connaissance du contenu d'un courriel, ne peut le faire sans prendre connaissance simultanément de son existence. La prise de connaissance et l'usage du contenu d'un courriel sont liés à la prise de connaissance et à l'usage de l'existence de ce courriel. »

Sans fournir une analyse approfondie des termes de la loi, la Cour de cassation constate donc de façon pragmatique que l'article 124 de la loi fait obstacle à la prise de connaissance du contenu de la communication électronique. Celui-ci est donc protégé par l'article 124 de la loi du 13 juin 2005[2].

1. Cass., 1er octobre 2009, R.G. n° C.08.0064.N, www.cass.be.
2. C'était également la position de C. DE TERWANGNE, J. HERVEG et J.-M. VAN GYSEGHEM, *in Le divorce et les technologies de l'information et de la communication*, Bruxelles, Kluwer, 2005, p. 46.

2.4. Les actes incriminés et la notion de caractère intentionnel

Il est question, dans les trois premiers alinéas de l'article 124, de prise de connaissance ou d'identification *intentionnelle*.

Les travaux préparatoires de la loi ne fournissent pas d'indication sur la façon d'interpréter ce caractère intentionnel dans ce contexte. Les travaux préparatoires du projet de loi ayant mené à l'adoption des articles 314*bis* et 259*bis* du Code pénal, dispositions qui participent au secret des communications électroniques et qui font également référence à l'exigence d'un élément intentionnel, indiquent, à ce propos, qu'une simple coïncidence ou indiscrétion ne suffit pas[1].

La jurisprudence dont nous avons connaissance et qui s'est prononcée sur la question opère une distinction qui s'inscrit dans ce même ordre d'idées, puisqu'elle va opposer la prise de connaissance fortuite à la prise de connaissance intentionnelle.

Ainsi, le Tribunal du travail de Bruxelles, dans une décision du 4 décembre 2007[2], distingue la découverte fortuite d'un courriel avec la consultation délibérée d'une telle communication dans un litige où l'employeur entendait établir l'existence d'une violation de l'obligation de non-concurrence dans le chef de son travailleur en produisant des courriels échangés par ce dernier avec des entreprises tierces. Le tribunal considéra qu'en l'absence du consentement du travailleur, il appartenait à l'employeur de prouver le caractère fortuit de la découverte des messages produits. Le tribunal constatera que cette preuve n'est pas rapportée, les explications données par l'employeur quant aux circonstances dans lesquelles il a pris connaissance des messages – lors d'un *back up*- n'étant pas convaincantes. Il subodora, compte tenu des tensions qui caractérisaient les relations entre les parties, le fait que l'employeur avait intentionnellement pris connaissance des courriers pour se ménager des preuves dans le cadre de la procédure[3].

Dans un jugement rendu le 19 mars 2008, le Tribunal du travail de Liège avait également à trancher si une prise de connaissance de courriels pouvait revêtir un caractère fortuit[4].

L'employeur avait licencié une secrétaire après avoir constaté que cette dernière communiquait des informations confidentielles appartenant à l'ancienne directrice de l'entreprise. Il invoquait avoir été intrigué par un courriel ouvert visible à l'écran. Ce courriel se trouvait dans la boîte de messagerie privée Yahoo de la travailleuse. Un

---

1. Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. parl.*, Sénat, 1992-1993, n° 841/1, p. 7.
2. Trib. trav. Bruxelles (24e ch.), 4 décembre 2007, *J.T.T.*, 2008, p. 179.
3. Pour un commentaire de cette décision, voy. K. Rosier, « Régularité de la preuve : tel est pris qui croyait prendre... », *B.S.J.*, 2008, n° 391, p. 5.
4. Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. n° 360.454, www.cass.be.

coup d'œil indiscret avait permis d'établir qu'il s'agissait d'un message échangé avec l'ancienne directrice. Le tribunal évoque qu'à cette occasion, plusieurs courriels ont été consultés et imprimés. Le tribunal estimera que la prise de connaissance initiale des faits est illégale, puisqu'elle est le fruit d'une démarche active (consultation et impression de courriels) intervenue sans le consentement de la travailleuse.

Dans une décision du 8 décembre 2010, la Cour du travail de Mons considère que, lorsqu'il est établi que la prise de connaissance d'une communication électronique est intervenue fortuitement, le caractère intentionnel de la découverte fait défaut et l'article 124 de la loi du 13 juin 2005 ne s'applique pas[1]. En l'espèce, le courriel litigieux découvert l'avait été par un collègue qui, en l'absence du travailleur concerné, licencié par la suite, avait consulté la boîte de courriers électroniques de ce dernier pour vérifier si le courriel attendu dans le cadre d'un projet lui avait été adressé. Il avait alors découvert un courriel se référant à un projet dont il n'avait pas connaissance et, pensant qu'il s'agissait d'une demande de remise de prix d'un nouveau client potentiel, l'avait ouvert.

On peut donc retenir de ces décisions qu'il faut faire une distinction entre un contrôle délibéré de l'employeur qui peut se limiter à une démarche de prise de connaissance active d'une communication électronique et la prise de connaissance purement fortuite.

Ceci étant, il convient de rester attentif au fait que l'alinéa 4 de l'article 124 sanctionne entre autres le fait de stocker ou de faire un usage quelconque de l'information, de l'identification ou des données obtenues *intentionnellement ou non*. L'utilisation d'une information obtenue de manière fortuite reste donc interdite.

2.5. Durée de la protection

Il est généralement admis, sans que cela transparaisse clairement du texte, que la protection de l'article 124 est applicable tant pendant la transmission qu'après que la transmission est achevée. Aussi, la question n'est jamais abordée de front en jurisprudence et en doctrine : il semble aller de soi que la consultation d'un courriel ayant déjà été ouvert dans la boîte de courriers électroniques du travailleur ou d'un *log file* faisant apparaître la liste des sites consultés à partir d'un poste de travailleur tombe sous le coup de l'application de l'article 124.

Une approche sous un angle historique de l'article 124 nous montre toutefois que ceci n'est pas évident.

1. C. trav. Mons (8e ch.), 8 décembre 2010, *J.L.M.B.*, 2011, p. 715 ; *Chron. D.S.*, 2011, p. 399, note O. Rijckaert.

En effet, la législation actuelle a pour origine la réglementation des télécommunications et était ancrée dans le monde de la téléphonie. À l'époque de la téléphonie, la question avait essentiellement trait aux données de communications liées à la facturation par exemple et qui restaient disponibles après la fin de la communication sans qu'il y ait eu écoute ou enregistrement par un tiers, tel l'employeur. À cet égard, il n'y avait pas de position tranchée sur la question en doctrine et en jurisprudence. Ainsi, certains auteurs étaient farouchement opposés à la communication de telles données par les opérateurs téléphoniques[1] à l'employeur, tandis que certaines décisions de jurisprudence n'y voyaient aucun obstacle[2].

Toutefois, avec l'apparition de nouveaux moyens de communication tels l'Internet et les courriers électroniques, les SMS, le champ d'application de cette protection s'est étendu et a inclus d'autres formes de communications qui se caractérisent par la rémanence non seulement d'une trace de la communication, mais surtout de son contenu.

Toujours est-il que c'est sans véritable réflexion à ce sujet ni état d'âme que la jurisprudence et la doctrine ont considéré la protection concernant ces traces laissées par la communication après la transmission achevée comme incluse dans le champ de la protection. En cela, la protection prévue à l'article 124 de la loi des communications électroniques se différencie de celle des articles 314*bis* et 259*bis* du Code pénal qui ne vaut que pendant la transmission.

3. Exceptions au secret des communications

3.1. Le consentement des personnes concernées par la communication

À l'instar des articles 314*bis* et 259*bis* du Code pénal, l'article 124 de la loi du 13 juin 2005 n'érige en infraction les actes repris dans son libellé que dans l'hypothèse où ils interviendraient sans le consentement des parties à la communication.

Dès lors, il convient de déterminer quels sont les consentements requis et quelles sont les exigences pour qu'un consentement soit pris en considération.

1. P. De Hert, « Schending van het (tele)communicatiegeheim in het beroepsleven », *R.D.S.*, 1995, n° 36 ; L. Arnou, « Het respecteren van telefoongeheim in België na het afluisterwet van 30 juni 1994 », *Computerr.*, 1995/4, p. 164.
2. Trib. trav. Bruxelles, 16 septembre 2004, R.G. n° 0353058, www.cass.be.

3.1.1. Quelles sont les personnes dont il convient d'obtenir le consentement ?

Bien que les termes utilisés dans l'article 124 soient extrêmement larges et puissent inclure les personnes visées par le contenu de la communication (« S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées [...] »), la doctrine[1] et la jurisprudence[2] retiennent généralement implicitement que les personnes visées sont les expéditeurs et les destinataires des messages.

Le fait que le consentement de toutes les parties à la communication soit requis rend illusoire, par exemple, dans le cadre de la relation de travail, la possibilité d'opérer des prises de connaissance de communications lorsqu'il y a des parties à la communication qui sont externes à l'entreprise. La situation peut être envisagée différemment lorsqu'il s'agit, par exemple, de connexions à l'Internet où il n'y a qu'une partie à la communication dont le consentement est requis – l'internaute –, pour autant que ce consentement puisse être considéré comme valable au regard des critères décrits sous la section suivante.

3.1.2. Quelles conditions le consentement doit-il remplir pour être valable ?

Le consentement doit être libre et spécifique et individuel.

Un consentement *libre*. La question du caractère libre se pose avec une acuité particulière dans le cadre d'une relation de travail qui suppose un lien de subordination entre le travailleur et l'employeur. Si le fait de se trouver dans un lien de subordination n'empêche pas *ipso facto* qu'un consentement puisse être librement donné par le travailleur, il convient d'être attentif aux circonstances dans lesquelles il est donné.

On constate des prises de position différentes quant à la possibilité d'obtenir un consentement libre dans ce contexte.

– Ainsi, la Commission de la protection de la vie privée a-t-elle estimé qu'était douteux le caractère libre du consentement de l'employé lorsque celui-ci, pour utiliser l'Internet – à quelque fin, personnelle ou professionnelle, que ce soit – n'a pas d'autre choix que de cliquer sur le bouton d'acceptation des conditions imposées par l'employeur afin d'avoir accès au réseau[3] et elle a depuis lors considéré

1. Voy., notamment, J.-P. Cordier et S. Becket, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondeau*, Louvain-la-Neuve, Anthemis, 2008, p. 85.
2. Pour des décisions concernant l'exigence d'un consentement du travailleur, voy., notamment, C. trav. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262 ; C. trav. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100 ; C. trav. Anvers (sect. Anvers), 15 décembre 2004, *Chron. D.S.*, 2006, p. 146 ; C. trav. Bruxelles (3e ch.), 10 février 2004, *Oriëntatie*, 2004, p. 3, note A. Vanoppen ; *Orientations*, 2006, p. 141 ; C. trav. Anvers (sect. Anvers), 1er octobre 2003, *J.T.T.*, 2004, p. 510 ; Trib. trav. Hasselt (1re ch.), 21 octobre 2002, *Chron. D.S.*, 2004, p. 197.
3. C.P.V.P., avis n° 13/03 sur le contrôle par l'employeur des données de communications de l'un de ses employés, 27 février 2003, p. 5, www.privacycommission.be.

dans une recommandation en 2012 que « le consentement du (des) travailleur(s) concerné(s) ne peut pas constituer la base légale autorisant un contrôle patronal des actes numériques accomplis par les travailleurs dans le cadre de la relation de travail ou à l'aide des outils de travail. En raison de force existant entre les parties, un consentement individuel des travailleurs concernés ne pourrait être considéré comme véritablement libre »[1]. Dans un même ordre d'idées, la Cour du travail de Bruxelles a jugé que le consentement d'une travailleuse obtenu par l'employeur pour consulter certains de ses courriels lors d'un entretien faisant état du trop grand nombre de courriels envoyés par celle-ci depuis son poste à des fins privées ne pouvait être considéré comme libre et éclairé, dès lors que celle-ci se trouvait sous pression au moment où elle avait donné son autorisation.

- En sens inverse, le Tribunal du travail de Liège a estimé qu'une travailleuse confrontée à une demande de consultation de ses courriels en présence d'un huissier pouvait valablement y consentir[2].

Un consentement *spécifique*. Qu'en est-il d'un possible consentement donné *a priori* sur le principe du contrôle lui-même ?

Le caractère spécifique du consentement peut faire obstacle à ce que celui-ci soit donné anticipativement et de manière générale. Dans les travaux préparatoires de la loi du 30 juin 1994 insérant les articles 314*bis* et 259*bis* du Code pénal, il est d'ailleurs spécifié qu'une clause par laquelle un employeur se réserverait le droit d'écouter des conversations téléphoniques de son employé serait inacceptable[3]. Il en résulte de ces considérations qu'un consentement obtenu de manière générale ne serait pas suffisant.

Un consentement *individuel*. Le consentement doit encore être individuel. À cet égard, si l'insertion au sein du règlement de travail, par exemple, de règles relatives à l'utilisation du courriel ou de l'Internet est parfaitement envisageable, il reste que l'on ne pourrait y inscrire, à notre estime, le principe d'une autorisation de l'employé à consulter ses courriels.

Quid d'un consentement *tacite* ? On peut encore se demander si le consentement doit être explicite ou s'il peut être tacite. Les travaux préparatoires de la loi du 30 juin

---

1. C.P.V.P., Recommandation d'initiative n° 08/2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, 2 mai 2012, pp. 36 et 37, www.privacycommission.be.
2. Il a toutefois estimé qu'en l'espèce, dès lors que cette demande était formulée parce que l'employeur avait constaté initialement des faits au moyen d'une consultation illicite et au mépris total du principe de loyauté dans l'exécution du contrat de travail, l'irrégularité initiale implique que toutes les démarches ultérieures visant à obtenir une preuve de ces faits sont entachées d'irrégularité (Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. n° 360.454, www.cass.be). Sur ce point, le tribunal rejoint la position adoptée par le Tribunal du travail de Bruxelles dans un jugement du 4 décembre 2007 qui avait considéré qu'« il ne saurait par ailleurs être recouru à d'autres modes de preuve, tels [que] des enquêtes, pour établir des éléments révélés par ces preuves acquises illégalement » (Trib. trav. Bruxelles (24e ch.), 4 décembre 2007, *J.T.T.*, 2008, p. 179).
3. Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. parl.*, Sénat, 1992-1993, séance du 1er septembre 1993, n° 843/1, p.8.

1994 insérant les articles 314*bis* et 259*bis* du Code pénal ne l'excluent pas[1]. La doctrine a relevé qu'il a été considéré qu'il y avait consentement tacite, mais indubitable, lorsqu'une conversation est menée par le biais d'un talk, de sorte que l'écoute du talk est nécessaire pour que la conversation puisse avoir lieu ou encore dans l'hypothèse où une secrétaire est chargée de noter ce qui était dit lors d'une conversation téléphonique et à ce titre en prend connaissance[2]. La Cour du travail d'Anvers a estimé, entre autres considérations, que le fait que la travailleuse licenciée pour avoir fait un usage intensif du courriel à des fins privées avait communiqué à son collègue son mot de passe emportait son consentement implicite pour que ce dernier consulte ses courriels[3]. Ceci étant, on relèvera, avec F. Hendrickx, qu'il ne suffit pas toutefois que la conversation ait lieu dans un cadre professionnel pour pouvoir en déduire l'existence d'un consentement[4]. Là encore, il y a lieu d'apprécier au cas par cas.

On le voit, la question du consentement reste délicate, tandis que nombre de décisions de jurisprudence insistent sur le fait que des données électroniques ne peuvent être produites sans *le consentement* du travailleur et/ou les autres parties à la communication et, à défaut, déclarent la preuve irrecevable[5].

Dans le cadre de l'application de l'article 124 dans les relations de travail, la Commission de la protection de la vie privée a préconisé que le consentement du travailleur soit sollicité par rapport à des modalités de contrôle négociées collectivement. En effet, dans sa Recommandation n° 1/2002 du 22 août 2002[6] : « En ce qui concerne les employés, une note de service ou le règlement de travail seul ne sont pas suffisants pour garantir le consentement libre de l'employé. Il s'agit de combiner le consentement individuel de l'employé avec la négociation d'un texte général à laquelle seront associés les représentants des employés [...] Le consentement obtenu par la mention des conditions d'enregistrements dans le règlement de travail ou le code de conduite, qui font l'objet d'une discussion au sein du conseil d'entreprise et contribuent ainsi au caractère libre du consentement, pourra par exemple être complété via un avenant au contrat de travail ou la signature d'un formulaire *ad hoc* par l'employé, garantissant ainsi le caractère individuel du consentement. »

---

1. Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. parl.*, Sénat, 1992-1993, séance du 1er septembre 1993,n° 843/1, p. 8, et n° 843/2, p. 10.
2. L. Arnou, « Uit respecteren van het telefoon geheim in België na de afluiterwet van 30 juni 1994 », *Computerr.*, 1995/4, 160.
3. C. trav. Anvers (sect. Anvers), 8 janvier 2003, R.G. n° 2020255, www.cass.be.
4. F. Hendrickx, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, p. 197.
5. C. trav. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262 ; C. trav. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100 ; C. trav. Anvers (sect. Anvers), 15 décembre 2004, *Chron. D.S.*, 2006, p. 146 ; C. trav. Bruxelles (3e ch.), 10 février 2004, *Oriëntatie*, 2004, p. 3, note A. Vanoppen ; *Orientations*, 2006, p. 141 ; C. trav. Anvers (sect. Anvers), 1er octobre 2003, *J.T.T.*, 2004, p. 510 ; Trib. trav. Hasselt (1re ch.) 21 octobre 2002, *Chron. D.S.*, 2004, p. 197 ; C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2001, p. 41 ; Trib. trav. Bruxelles (12e ch.), 22 juin 2000, *Computerr.*, 2001/6, p. 312.
6. C.P.V.P., Recommandation n° 01/2002 du 22 août 2002 relative à l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, www.privacycommission.be

Si cette approche peut offrir une solution pour le contrôle des connexions à l'Internet des travailleurs y ayant consenti dans la mesure où celles-ci n'impliquent aucune communication avec un tiers et des courriels ou autres communications électroniques entre personnes ayant accepté le contrôle, il demeure qu'elle reste imparfaite en ce qui concerne les communications impliquant des tiers. Certes, la transparence et la prévisibilité d'une solution négociée sont de nature à désamorcer certains conflits, mais il demeure qu'aux termes de la loi, le consentement de toutes les parties concernées est requis[1]. Si l'on peut concevoir d'obtenir le consentement de l'employé partie à la communication, qu'en est-il du tiers qui, en qualité de destinataire ou d'expéditeur, est partie à la communication ? Il nous semble que l'exigence d'un consentement véritable interdit d'envisager de se limiter à informer les destinataires de courriers électroniques du fait que tous les courriels adressés par l'employé sont susceptibles d'être lus ou conservés par l'employeur.

3.2. Les exceptions prévues à l'article 125 de la loi

3.2.1. Le texte légal

L'article 125 de la loi prévoit des exceptions à ces interdictions dans les hypothèses suivantes :

> « 1er. Les dispositions de l'article 124 de la présente loi et les articles 259*bis* et 314*bis* du Code pénal ne sont pas applicables :
>
> 1° lorsque la loi permet ou impose l'accomplissement des actes visés ;
>
> 2° lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques ;
>
> 3° lorsque les actes sont accomplis en vue de permettre l'intervention des services de secours et d'urgence en réponse aux demandes d'aide qui leur sont adressées ;
>
> 4° lorsque les actes sont accomplis par l'Institut[2] sur ordre d'un juge d'instruction et/ou dans le cadre de sa mission générale de surveillance et de contrôle ;

1. C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2001, p. 41.
2. Il est fait référence à l'Institut belge des services postaux et des télécommunications tel que visé à l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (*cf.* art. 2, 1°, de la loi du 13 juin 2005).

5° lorsque les actes sont accomplis par le service de médiation pour les télécommunications ou à la demande de celui-ci dans le cadre de ses missions légales de recherche et ne concernent pas l'écoute de communications ;

5°/1 lorsque les actes sont accomplis par les agents habilités par le ministre qui a l'économie dans ses attributions, dans le cadre de leurs missions légales de recherche et ne concernent pas l'écoute de communications ;

5°/2 lorsque les actes sont accomplis par la Commission d'éthique pour les télécommunications ou son secrétariat ou à la demande de l'un d'eux dans le cadre de leurs missions légales de recherche et ne concernent pas l'écoute de communications ;

6° lorsque les actes sont accomplis dans le seul but d'offrir des services à l'utilisateur final consistant à empêcher la réception de communications électroniques non souhaitées, à condition d'avoir reçu l'autorisation de l'utilisateur final à cet effet.

§ 2. Le Roi fixe, après avis de la Commission de la protection de la vie privée et de l'Institut, par arrêté délibéré en Conseil des ministres, les modalités et les moyens à mettre en œuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques ».

Mise à part la première hypothèse de l'article 125 qui envisage le cas où l'accomplissement des actes est permis ou imposé par la loi, les autres exceptions visent donc tantôt à permettre l'accomplissement des actes à certaines finalités (intervention du service d'urgence, vérification du bon fonctionnement du réseau ou exécution d'un service de communication électronique, fourniture d'un service de lutte contre le *spam*[1]), tantôt à permettre à certaines autorités de mener à bien les missions qui leur sont confiées (voy. les alinéas 4° et 5° de l'article 125).

Nous ne nous étendrons pas sur ces hypothèses et n'évoquerons brièvement que les deux premiers cas de figure envisagés par la loi, qui nous paraissent mériter davantage de commentaires. Nous aurons l'occasion de revenir sur l'obligation de collaboration mise à charge des opérateurs et d'autres fournisseurs dans le chapitre 5.4, section 4.7.

1. Dans un avis de 2004, la Commission de la protection de la vie privée estimait qu'il fallait opérer une distinction entre de simples courriers non sollicités et une attaque via envoi massif de courriels visant à provoquer la saturation d'un système ou d'un réseau. Dans ce dernier cas, l'opérateur devrait pouvoir prendre des mesures visant à assurer le bon fonctionnement du réseau, sans obtenir préalablement le consentement des utilisateurs sur la base de l'article 125, 2° (C.P.V.P., avis 2004/08 relatif à l'avant-projet de loi relative aux communications électroniques, 14 juin 2004, p. 8, www.privacycommission.be).

3.2.2. Les actes permis ou imposés par la loi

La première question que l'on peut se poser à propos de l'interprétation à donner à cette exception est celle du sens dans lequel le terme « loi » doit être entendu. Ni la loi ni les travaux préparatoires n'en disent mot. À notre estime, il faut entendre le terme loi au sens formel. En effet, si l'on a égard à l'article 22 de la Constitution, il nous faut rappeler que celui-ci réserve au législateur seul le droit de restreindre le droit à la protection de la vie privée. Or une exception à l'article 124 induit assurément une telle atteinte. C'est pourquoi il nous semble que seul un texte de valeur législative est susceptible de pouvoir éventuellement prévoir ou permettre l'accomplissement des actes dont question.

Une difficulté peut toutefois surgir quant à l'exigence de précision requise par rapport à la loi. En effet, il existe peu de dispositions légales qui permettent ou imposent spécifiquement l'accomplissement des actes visés aux articles 124 de la loi du 13 juin 2005 et aux articles 314*bis* ou 259*bis* du Code pénal. Par exemple, on peut penser à l'article 88*bis* du Code d'instruction criminelle qui permet, à certaines conditions, le repérage de télécommunications ou la localisation de l'origine ou de la destination de télécommunications[1] ou, encore, à l'article 126 de la loi du 13 juin 2005 qui a trait à l'obligation faite aux opérateurs d'enregistrer et de conserver les données de trafic et les données d'identification d'utilisateurs finals en vue de leur réutilisation dans le cadre de la poursuite et la répression d'infractions pénales[2].

D'autres dispositions, si elles ne mentionnent pas spécifiquement des données de communications, les englobent certainement. On peut penser au décret wallon du 6 décembre 2001 relatif aux archives publiques qui impose la conservation des archives, ce terme étant défini à l'article 1er du décret comme étant « l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel ». Ceci nous semble devoir inclure les communications électroniques. Un autre exemple peut encore être trouvé à l'article 8, § 1er, alinéa 4, de la loi du 11 mars 2003 relative sur certains aspects juridiques des services de la société de l'information. Cette disposition permet au prestataire d'archiver une copie du contrat passé. Étant donné qu'il s'agit de contrats conclus dans le cadre du commerce électronique, on peut en déduire que l'enregistrement du contrat peut impliquer l'enregistrement de données de communications du cocontractant.

Hors ces hypothèses, il y a matière à interprétation.

À titre d'illustration de cette problématique, nous relevons que la question s'est posée de savoir si la loi du 3 juillet 1978 relative aux contrats de travail – en particulier

1. Voy. également les articles 46*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle qui traitent également du repérage, de la localisation, des écoutes, de la prise de connaissance et de l'enregistrement des communications.
2. *Cf.*, à ce sujet, chapitre 5.4, *infra*.

l'article 17, 1° et 2°, de la loi consacrant le pouvoir d'autorité de l'employeur – pouvait constituer une base légale suffisante au regard de l'article 109*ter*E de la loi Télécom et la disposition qui y a été substituée, l'article 125 de la loi du 13 juin 2005. On constate une évolution à ce sujet.

Il semblait se dégager une opinion majoritaire pour rejeter l'idée que ces dispositions auraient un caractère suffisamment précis pour constituer une base légale suffisante[1]. La Commission de la protection de la vie privée avait d'ailleurs fait sienne cette position en constatant que « la surveillance électronique des travailleurs ne peut pas être assimilée sans plus à une forme "moderne" d'exercice de l'autorité »[2], avant de changer de position dans une Recommandation n° 08/2012, sur laquelle nous reviendrons.

En sens contraire, M. Lauvaux, V. Simon et D. Stas de Richelle relèvent toutefois que, dans le cadre de l'examen de l'article 314*bis* du Code pénal, le Tribunal du travail de Bruxelles[3] et la Cour du travail de Gand[4] ont estimé ces articles suffisants pour autoriser une ingérence de l'employeur dans la vie privée du travailleur[5]. Nous avons également relevé des décisions en ce sens à propos de l'article 109*ter*D, remplacé par l'article 124 de la loi du 13 juin 2005[6], et des décisions du Tribunal du travail de Bruxelles qui a estimé que l'application de l'article 16 de la loi du 3 juillet 1978 en ce qu'il impose à l'employeur d'assurer le respect des convenances et des bonnes mœurs sur le lieu de travail constitue une « autorisation légale » d'exercer un contrôle[7].

Dans une Recommandation n° 08/2012, la Commission de la protection de la vie privée change sa position sur la question et estime désormais que l'employeur peut bénéficier de l'exception prévue à l'article 125, § 1er, 1°, moyennant le respect de certaines conditions, et ce, sur la base de la motivation suivante :

---

1. Comme le constatent J.-P. Cordier et S. Bechet (« La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, pp. 85 et 86), et O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, p. 51. Ainsi, selon F. Hendrickx, l'article 17, 2°, de la loi sur le contrat de travail n'offre aucune base suffisamment précise et claire pour en déduire la possibilité d'utiliser des caméras de surveillance, de procéder à des examens médicaux ou à des écoutes téléphoniques ou encore à la fouille de membres du personnel ou de toute autre atteinte du même ordre (F. Hendrickx, *Electronisch toezicht op het werk, Internet en camera's*, Ced. Samson, 2000, p. 308) ; voy., également, J. Dumortier, « Internet op het werk, controlerechten van de werkgever », *Orientatie*, 2000 p. 38 ; P. Leduc, « Le contrôle des communications données et reçues par le travailleur », *Ubiquité*, 2000/5, p. 47 ; J.-P. Lacomble et C. Preumont, « Ontslag wegens dringende reden en bescherming van privacy », *Cah. jur.*, 2005, p. 96 ; C. trav. Bruxelles (3e ch.), 8 avril 2003, *Chron. D.S.*, 2005, p. 208 ; *contra* : R. De Corte, « Surfen op het werk : een kwestie van n'et uitg'jden », *Juristenkrant*, 7 novembre 2000, p. 7, et F. Lagasse, « La vie privée et le droit du travail », *Chron. D.S.*, 1997, p. 425.
2. C.P.V.P., avis n° 13/03 sur le contrôle par l'employeur des données de communications de l'un de ses employés, 27 février 2003, p. 9, www.privacycommission.be.
3. Trib. trav. Bruxelles, 16 septembre 2004, *J.T.T.*, 2005, p. 61.
4. C. trav. Gand, 9 mai 2005, inédit, R.G. n° 269/02.
5. M. Lauvaux, V. Simon et D. Stas de Richelle, *Criminalité au travail*, Bruxelles, Kluwer, 2007, p. 102.
6. C. trav. Mons, 25 novembre 2009, *R.D.T.I.*, 2009, p. 229, note K. Rosier et S. Gilson.
7. Trib. trav. Bruxelles (12e ch.), 22 juin 2000, *Computerr.*, 2001/6, p. 11 ; Trib. trav. Bruxelles, 6 septembre 2001, *J.T.T.*, 2002, p. 52.

« Les articles 2, 3, 4 et 5 de la loi relative aux contrats de travail prévoient, comme un élément essentiel du contrat, l'autorité de l'employeur (c'est-à-dire ses pouvoirs de direction et de surveillance).

L'article 16 de la loi relative aux contrats de travail prévoit également que les deux parties se doivent le respect et des égards mutuels. L'article 17 de cette même loi indique que le travailleur est obligé d'exécuter son travail avec soin, probité et conscience et d'agir conformément aux ordres et aux instructions de son employeur.

La Commission estime que ces dispositions, ou des dispositions similaires dans la fonction publique, ainsi que les directives établies dans la LVP et dans la C.C.T. n° 81, sont suffisamment claires pour définir dans quelle mesure l'employeur dispose d'un quelconque droit de contrôle. Aux yeux de la Commission, ces dispositions, lues conjointement, constituent une autorisation légale au sens de l'article 125, § 1, 1°, de la loi relative aux communications électroniques, ce qui exclut toute violation de l'article 124 de la loi relative aux communications électroniques, pour autant que l'employeur respecte les trois principes de base de ces législations, dont le respect est jugé essentiel pour la protection de la vie privée des travailleurs lors d'un traitement de leurs données à caractère personnel : le principe de finalité, le principe de proportionnalité et le principe de transparence »[1].

Sans prétendre à l'exhaustivité, on peut encore citer, à titre d'exemple, un autre cas dans lequel on pourrait envisager soutenir qu'une loi permette ou impose implicitement l'accomplissement des actes prévus à l'article 124.

Ainsi, la Commission de la protection de la vie privée a-t-elle estimé que l'article 16 de la loi du 8 décembre 1992 qui impose au responsable du traitement d'assurer la sécurité des données à caractère personnel implique de prendre les mesures techniques nécessaires pour assurer la sécurité des systèmes informatiques. Dans cette perspective et à cette fin, l'enregistrement de loggings de données de communications par le responsable du traitement est admissible, voire souhaitable, selon la Commission[2].

3.2.3. Les mesures techniques

La seconde exception prévue à l'article 125 ne permet que l'accomplissement de mesures d'ordre strictement technique lorsque les actes visés sont accomplis dans

1. C.P.V.P., Recommandation d'initiative n° 08/2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, 2 mai 2012, p. 36, www.privacycommission.be.
2. C.P.V.P., avis 18/2005 relatif à un projet d'arrêté du Gouvernement de la Communauté française relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII, 9 novembre 2005, pp. 3 et 4, www.privacycommission.be.

le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques.

Certains auteurs[1] ont fait remarquer, à propos de la même exception qui était déjà prévue à l'article 109*ter*E, § 1er, 1°, que celle-ci vise en réalité des interventions sur le réseau public de communications, et ce, en se fondant sur les travaux préparatoires de la loi[2]. Interpellé sur ce qu'il adviendrait dans l'hypothèse où l'employé d'un opérateur effectuerait d'initiative des écoutes téléphoniques – le libellé de la disposition tel que proposé évoquait *des actes visés posés pour assurer un service de télécommunication* –, le ministre de l'époque avait précisé qu'étaient visés les actes *ayant pour but* d'assurer ledit service.

D'autres auteurs ont, en revanche, interprété l'exception dont question comme permettant des interventions nécessitées sur le réseau de l'entreprise par l'entreprise[3], de sorte que ce serait la finalité qui importerait davantage que l'identité de la personne qui accomplit l'acte ou le type de réseau (public ou privé) concerné[4].

Cette seconde interprétation ne nous semble pas contraire aux termes de la loi, puisque les définitions des concepts de « réseau de communications électroniques » ou de « services de communications électroniques » sont tellement larges qu'elles peuvent inclure un réseau strictement privé[5].

3.3. Les exceptions prévues à l'article 128 de la loi du 13 juin 2005 sur les communications électroniques

3.3.1. L'enregistrement de communications commerciales

L'article 128, § 1er, de loi du 13 juin 2005 relative aux communications électroniques prévoit la possibilité d'enregistrer une communication électronique dès lors que celle-ci est effectuée dans le cadre de transactions commerciales licites et que l'enregistrement intervient dans le but de faire preuve d'une transaction commerciale ou d'une autre communication professionnelle. Cet enregistrement est toutefois soumis

1. J. Dumortier, « Internet op het werk, controlerechten van de werkgever », *Oriëntatie*, 2000, p. 38 ; Th. Claeys et D. Dejonghe, « Gebruik van *e-mail* en internet op de werkplaats en controle door de werkgever », *J.T.T.*, 2001, p. 128.
2. Projet de loi portant réforme de certaines entreprises publiques économiques, *Doc. parl.*, Chambre, 1990-1991, n° 1287/10-89/90, p. 174.
3. O. Ruckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, pp. 51 et 52 ; H. Barth, « Contrôle de l'employeur de l'utilisation "privée" que font ses travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *J.T.T.*, 2002, p. 173.
4. On notera qu'une des finalités de contrôle admises dans la C.C.T. n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau opère clairement un glissement vers des mesures accomplies sur le réseau de l'entreprise par l'entreprise. En son article 5, § 1er, 3°, le texte de la C.C.T. n° 81 prévoit que le contrôle de données de communications électroniques en réseau est autorisé lorsqu'il est accompli en vue d'assurer « la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ».
5. *Cf.* chapitre 5.2, section 1., *supra*.

à des exigences strictes : toutes les parties impliquées dans la communication doivent avoir été préalablement informées de l'enregistrement, des objectifs précis de ce dernier, ainsi que de la durée de stockage de l'enregistrement. De plus, les données visées dans cette disposition doivent être effacées au plus tard à la fin de la période pendant laquelle la transaction peut être contestée en justice. Enfin, l'article 128 précise que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel reste applicable aux traitements de données à caractère personnel qu'implique cet enregistrement.

Il paraît, toutefois, extrêmement difficile d'assurer une information préalable de toutes les personnes concernées sachant que, parfois, le courrier électronique que l'entreprise souhaitera conserver lui sera adressé par un tiers sans qu'elle ait pu l'informer quant à sa politique d'enregistrement des courriers électroniques. Par ailleurs, l'autorisation du seul enregistrement peut être insuffisante si la prise de connaissance n'est pas autorisée également. Enfin, la conciliation de cette disposition avec la loi du 8 décembre 1992 suscite également des questions. Par exemple, le libellé de l'article 128 n'indique pas clairement si l'obligation d'information de l'article 9 de la loi du 8 décembre 1992 reste applicable ou si elle est remplacée par celle décrite dans la disposition[1].

Cette disposition paraît donc plus adaptée à l'enregistrement systématique de courriers électroniques dans le cadre d'une activité bancaire, par exemple, où les utilisateurs d'un service bancaire à distance sont prévenus que les communications électroniques échangées avec la banque seront automatiquement enregistrées. En revanche, son application dans l'ensemble du secteur commercial et professionnel de manière plus générale, comme le suggère son texte, nous paraît difficilement envisageable.

3.3.2. L'enregistrement de communications téléphoniques dans le cadre de call centers

L'article 128, § 2, de la loi du 13 juin 2005 crée une seconde dérogation aux articles 259*bis* et 314*bis* du Code pénal en admettant la prise de connaissance et l'enregistrement de communications électroniques et des données de trafic, qui visent uniquement à contrôler la qualité du service dans les *call centers* moyennant respect de certaines conditions.

Si cette disposition fait tomber l'exigence de l'obtention du consentement préalable de toutes les parties, elle maintient toutefois que les personnes qui travaillent dans le *call center* doivent être informées au préalable du but précis de cette opération, de la possibilité de prise de connaissance et d'enregistrement et de la durée de conserva-

1. Voy., à cet égard, les développements sur les difficultés liées à l'application cumulative des deux lois dans le chapitre 5.1, section 3., *supra*.

tion de la communication qui ne peut excéder un mois. L'article 128, § 2, indique expressément que ceci est sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée.

3.4. L'état de nécessité

La doctrine a évoqué la possibilité de se prévaloir de l'état de nécessité pour poser des actes en principe prohibés du fait du secret des communications électroniques[1]. Il s'agirait de justifier *a posteriori* le non-respect de ces dispositions par cette cause générale de justification en droit pénal. Comme le rappelle O. Rijckaert, seules des situations extrêmes pourraient éventuellement permettre l'invocation de cette cause de justification et l'auteur de citer la commission par le travailleur d'une infraction d'une gravité extrême (telle que la réception ou la distribution d'images pédopornographiques ou la divulgation de secrets de fabrique)[2].

4. Vers une atténuation des principes dans certains contextes ?

Nous ne pouvons évoquer le secret des communications électroniques sans signaler que, dans certains contextes, se dessine ou s'est affirmée une tendance à atténuer la rigueur du secret des communications.

Nous pensons tout d'abord au contexte des relations entre époux eu égard à un certain droit à la curiosité qui a été invoqué pour justifier des ingérences dans le droit au respect de la vie privée entre époux[3]. Cette plus grande souplesse dans l'appréciation des règles applicables s'est manifestée dans la prise de connaissance de courriers et de courriers électroniques[4].

Dans un arrêt du 27 janvier 2000[5], la Cour de cassation a considéré que ni l'article 8 CEDH ni l'article 29 de la Constitution relatif à l'inviolabilité des lettres ne faisaient obstacle à ce que des lettres régulièrement entrées en possession d'une partie à un litige en matière de divorce ne puissent être produites dans le cadre de cette procé-

1. F. Hendrickx, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, pp. 242 et 243.
2. O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, p. 52.
3. Voy., p. ex., Cour eur. D.H., L.L. c. France, 10 octobre 2006, req. n° 7508/02 ; Cour eur. D.H., N.N. et T.A. c. Belgique, 13 mai 2008, req. n° 65097/01.
4. Voy., à cet égard, C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication*, Bruxelles, Kluwer, 2005, p. 66.
5. Cass. (1re ch.), 27 janvier 2000, *Pas.*, I, 2000, p. 224.

dure. Ce principe a été étendu aux communications électroniques dans des décisions de fond. Ainsi, la Cour d'appel d'Anvers a-t-elle considéré, dans un arrêt du 21 avril 2010, que « [l]es époux disposent d'un certain droit à la curiosité qui les autorise à vérifier le respect des droits du mariage, et, en cas de violation de ces droits, à s'en réserver une preuve. Un époux peut dès lors utiliser en justice du courrier appartenant à son conjoint, à condition d'en être entré en possession de manière licite. Ces principes valent aussi pour les communications électroniques »[1]. On pointera également un arrêt de la Cour d'appel de Bruxelles qui résume les principes appliqués dans ce contexte de relations entre époux comme suit : « En droit commun, des documents privés tels que des courriers ou des courriels ne peuvent être déposés par des tiers. Toutefois, la doctrine et la jurisprudence ont admis une exception dans le cadre des procédures en divorce à la double condition que ni l'auteur ni le destinataire ne peuvent être soumis au secret professionnel et que le conjoint qui produit les documents privés ne peut avoir utilisé de moyen illicite pour entrer en leur possession »[2].

L'atténuation des principes viserait donc la prise de connaissance et l'utilisation de communications électroniques si l'entrée en possession est licite. On peut penser, par exemple, à une communication qui se trouverait dans une boîte librement accessible aux deux époux ou une communication portée à la connaissance d'un époux par un tiers. Il est à noter qu'une partie de la doctrine considère d'ailleurs de façon plus générale qu'il faut distinguer la preuve illicite en soi (tel un faux en écriture constitué à des fins probatoires) et la preuve obtenue illicitement (p. ex., preuve obtenue en violation du secret professionnel)[3]. Selon ces auteurs, les preuves appartenant à la première catégorie seraient, en toute hypothèse, irrégulières, tandis que les preuves obtenues de manière illicite ne seraient irrégulières que lorsqu'elles sont produites par une personne, impliquée directement ou indirectement dans l'irrégularité commise.

Un second terrain d'infléchissement du secret des communications est celui des relations de travail. La diversité des solutions jurisprudentielles dans l'interprétation et la portée donnée au secret des communications[4], notamment au regard d'autres dispositions, a mis en évidence le caractère très (voire trop) rigoureux de l'article 124 dans le contexte des relations de travail, puisque l'interdiction de prise de connais-

1. Anvers (3e ch.), 21 avril 2010, *T. Fam.*, 2011, p. 223, note C. Van Roy, « De machtiging tot afzonderlijke verblijfplaats fnukt het recht op nieuwsgierigheid ». L'arrêt précisait toutefois que, « [c]ependant, ce droit à la curiosité n'est plus valable après que les époux aient été autorisés par un juge à résider séparément. En l'espèce, dès lors que l'époux s'est procuré les missives électroniques échangées entre son épouse et des tiers après la date de la séparation judiciaire, ces documents ne peuvent servir de preuve dans le litige opposant les parties ».
2. Bruxelles (3e ch.), 7 novembre 2011, *Rev. trim. dr. fam.*, 2012, p. 164.
3. B. Allemeersch et S. Ryelandt, « Licéité de la preuve en matière civile : un clone pour "Antigoon" », *J.T.*, 2012, p. 166 et réf. citées ; D. Mougenot, « *Antigone* face aux juges civils. L'appréciation des preuves recueillies de manière illicite ou déloyale dans les procédures civiles », *D.A.O.R.*, 2011, p. 240 ; B. Allemeersch et P. Schollen, « Behoorlijk bewijs in burgerlijke zake – Over de geoorloofdheidsvereiste in the burgerlijk bewijsrecht », *R.W.*, 2002-2003, pp. 41 et s.
4. Voy. K. Rosier, « Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée », *R.D.T.I.*, 2012, nos 48 et 49, pp. 127 à 146 ; K. Rosier, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, 2009, n° 35, pp. 126 à 140.

sance des communications vaut également pour celles que l'on pourrait qualifier de « professionnelles ». Appliqué dans toute sa rigueur, l'article 124 est générateur d'obstacles pour assurer la continuité des prestations (accès aux communications en cas d'absence, de départ ou de décès d'un travailleur) et pour la gestion de la documentation de la vie économique de l'entreprise. On a vu que l'article 128 tel que rédigé n'était pas d'une grande utilité pour la prise de connaissance des courriers électroniques, ne serait-ce que pour la gestion des preuves des transactions commerciales.

C'est dans ce contexte que nous pointions une évolution de la position de la Commission de la protection de la vie privée concernant l'interprétation à donner à l'article 124. Dans une Recommandation publiée en 2012, la Commission défend une interprétation plus souple du cadre légal applicable afin de permettre une prise de connaissance et un contrôle des communications électroniques « raisonnable » eu égard au contexte de la relation de travail[1]. Il s'agit donc de défendre un raisonnement permettant de valider certaines prises de connaissance de communications électroniques, ce qui constitue un revirement en la matière[2].

5. Sanctions

Le non-respect de l'article 124 est sanctionné pénalement. L'article 145 du Code pénal prévoit :

> « § 1er. Est punie d'une amende de 50 à 50 000 EUR, la personne qui enfreint les articles 32, 33, 35, 41, 42, 114, 124, 127 et les arrêtés pris en exécution des articles 32, 39, § 3, 47 et 127.
>
> § 2. Est punie d'une amende de 200 à 2 000 EUR et d'une peine d'emprisonnement de huit jours à un an ou d'une de ces peines seulement, la personne qui enfreint l'article 39, § 1er, et les arrêtés pris en exécution de l'article 16.

1. C.P.V.P., Recommandation d'initiative n° 08/2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, 2 mai 2012, www.privacycommission.be.
2. Voy. C.P.V.P., Recommandation n° 01/2002 du 22 août 2002 relative à l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, www.privacycommission.be

§ 3. Est punie d'une amende de 500 à 50 000 EUR et d'une peine d'emprisonnement d'un à quatre ans ou d'une de ces peines seulement :

1° la personne qui réalise frauduleusement des communications électroniques au moyen d'un réseau de communications électroniques afin de se procurer ou de procurer à autrui un avantage illicite ;

2° (abrogé)

3° la personne qui installe un appareil quelconque destiné à commettre une des infractions susmentionnées, ainsi que la tentative de commettre celles-ci.

§ 3*bis*. Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communication électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci.

§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, 33, 35 et 37 est toujours prononcée ».

À notre connaissance toutefois, il y a peu de poursuites pénales sur la base de cette disposition. La violation de celle-ci est davantage invoquée dans le cadre d'une argumentation sur la recevabilité de la preuve[1] et/ou dans le cadre d'une demande de dommages et intérêts pour violation du droit au respect de la vie privée[2].

Il reste également possible d'envisager l'accomplissement des actes prohibés sous l'angle d'un traitement de données. Cela a, par exemple, été appliqué par les juridictions sociales dans le cadre de contrôles opérés par un employeur sur des communications électroniques d'un travailleur[3].

1. C. trav. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262 ; C. trav. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100 ; C. trav. Anvers (sect. Anvers), 15 décembre 2004, *Chron. D.S.*, 2006, p. 146 ; C. trav. Bruxelles (3e ch.), 10 février 2004, *Oriëntatie*, 2004, p. 3, note A. Vanoppen ; *Orientations*, 2006, p. 141 ; C. trav. Anvers (sect. Anvers), 1er octobre 2003, *J.T.T.*, 2004, p. 510 ; Trib. trav. Hasselt (1re ch.) 21 octobre 2002, *Chron. D.S.*, 2004, p. 197 ; C. trav. Bruxelles (3e ch.), 14 octobre 2011, R.G. n° 2010/AB/1029, www.cass.be.
2. Voy., p. ex.,.C. trav. Mons (8e ch.), 8 décembre 2010, *J.L.M.B.*, 2011, p. 715 ; *Chron. D.S.*, 2011, p. 399, note O. Rijckaert.
3. Voy., p. ex., Trib. trav. Liège, (10e ch.), 24 février 2005, inédit, R.G. n° 327.207 ; C. trav. Bruxelles, 8 avril 2003, *Chron. D.S.*, 2005, p. 208 ; C. trav. Mons (8e ch.), 8 décembre 2010, *J.L.M.B.*, 2011, p. 715 ; *Chron. D.S.*, 2011, p. 399, note O. Rijckaert.

CHAPITRE 5.4.
LA (RÉ)UTILISATION DES DONNÉES DE TRAFIC ET DES DONNÉES DE LOCALISATION

En marge des dispositions qui consacrent le secret des communications électroniques, les articles 122 et 123 règlent l'utilisation qui peut être faite des données traitées par les opérateurs pour fournir le service de communications électroniques.

Ces dispositions sont donc, nous semble-t-il, dérogatoires par rapport à l'article 124, puisqu'elles vont permettre, voire imposer, dans les limites qu'elles définissent, l'accomplissement d'actes interdits par l'article 124 de la loi du 13 juin 2005. Le libellé de l'alinéa 3 de l'article 124 de la loi confirme d'ailleurs cette interprétation, puisqu'il prévoit l'interdiction de prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne, *sans préjudice de l'application des articles 122 et 123.*

1. Les dispositions légales concernées : les articles 122 et 123 de la loi du 13 juin 2005

L'article 122 de la loi prévoit :

> « § 1er. Les opérateurs suppriment les données de trafic concernant les abonnés ou les utilisateurs finals de leurs données de trafic ou rendent ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication.
>
> L'alinéa 1er s'applique sans préjudice du respect des obligations de coopération, prévues par ou en vertu de la loi, avec :
> - les autorités compétentes pour la recherche ou la poursuite d'infractions pénales ;
> - le service de médiation pour les télécommunications pour la recherche de l'identité de toute personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques[1] ;

1. Voy. arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

- les services de renseignement et de sécurité dans le cadre de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité[1].

§ 2. Par dérogation au § 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs stockent et traitent les données suivantes :
- l'identification de la ligne appelante ;
- les adresses relatives à l'abonné et au lieu de raccordement, ainsi que le type d'équipement terminal ;
- le nombre total d'unités à facturer pour la période de facturation ;
- l'identification de la ligne appelée ;
- le type d'appel, l'heure à laquelle l'appel a commencé, la durée de l'appel ou la quantité de données transmises ;
- la date de la communication ou du service ;
- d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.

Sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, l'opérateur informe, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent :
- des types de données de trafic traitées ;
- des objectifs précis du traitement ;
- de la durée du traitement.

Le traitement des données énumérées à l'alinéa 1er, est seulement autorisé jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.

§ 3. Par dérogation au § 1er et dans le seul but d'assurer le marketing des services de communications électroniques propres ou des services à données de trafic ou de localisation, les opérateurs ne peuvent traiter les données visées au § 1er qu'aux conditions suivantes :

1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci en vue du traitement :
   a) des types de données de trafic traitées ;
   b) des objectifs précis du traitement ;
   c) de la durée du traitement.

1. Voy. arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité.

2° L'abonné ou, le cas échéant, l'utilisateur final, a, préalablement au traitement, donné son consentement pour le traitement.

Par consentement pour le traitement au sens du présent article, on entend la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées.

3° L'opérateur concerné offre gratuitement à ses abonnés ou ses utilisateurs finals la possibilité de retirer le consentement donné de manière simple.

4° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question ou pour l'action de marketing en question.

Ces conditions sont d'application sous réserve des conditions complémentaires découlant de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

§ 4. Par dérogation au § 1er, les données peuvent être traitées pour déceler des fraudes éventuelles.

Les données sont communiquées aux autorités compétentes en cas de délit.

§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des clients, de détecter les fraudes, du marketing des services de communications électroniques propres ou de la fourniture de services à données de trafic ou de localisation.

Le traitement est limité à ce qui est strictement nécessaire à l'exercice de telles activités.

§ 6. L'Institut, l'Autorité belge de la concurrence, les juridictions de l'ordre judiciaire et le Conseil d'État peuvent, dans le cadre de leurs compétences, être informés des données de trafic et de facture pertinentes en vue du règlement de litiges, parmi lesquels des litiges relatifs à l'interconnexion et la facturation. »

2. Les destinataires des articles 122 et 123

2.1. Les personnes tenues de respecter ces dispositions : les opérateurs

Une différence notable par rapport aux dispositions envisagées dans le chapitre 5.3 *supra* est que les articles 122 et 123 ne s'adressent principalement qu'aux opérateurs[1]. Ceci dit, on verra que pour certaines finalités d'utilisation, la possibilité de traitement n'est réservée qu'à certains opérateurs (les opérateurs de réseaux mobiles), tandis que certaines obligations de traitement (en matière de rétention de données) peuvent être mises à charge de personnes qui ne sont pas des opérateurs au sens de la loi, mais des fournisseurs de services de communications électroniques.

2.2. Les personnes bénéficiant de ces dispositions : les abonnés et utilisateurs finals

Les bénéficiaires des règles sont d'ailleurs définis par rapport à la notion d'« abonnés » et d'« utilisateurs finals » qui renvoient à la notion du service de communication électronique.

Ces concepts sont notamment utilisés dans la loi pour définir envers qui certaines obligations imposées aux opérateurs, telles qu'un devoir d'information concernant les traitements mis en œuvre, doivent être respectées.

L'abonné[2] est le cocontractant, mais il n'est pas toujours la personne qui utilisera *in fine* le service et adressera ou recevra des communications électroniques via ce service. C'est pourquoi la loi vise en certaines dispositions l'utilisateur[3] ou l'utilisateur final[4].

Comme nous l'avons évoqué au sein du chapitre 5.1, section 3.2. L'articulation entre la loi du 13 juin 2005 et la loi du 8 décembre 1992., le recours à ces concepts n'élimine pas toute difficulté quant à la détermination de la personne à qui devra être fournie l'information ou dont le consentement est requis.

---

1. Sur cette notion, voy. chapitre 5.2, section 1, *supra*.
2. L'abonné est défini par l'article 2, 15°, de la loi comme étant « toute personne physique ou morale qui utilise un service de communications électroniques en exécution d'un contrat passé avec un opérateur ».
3. L'utilisateur est défini par l'article 2, 12°, de la loi comme étant « une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public ».
4. L'utilisateur final est défini par l'article 2, 13°, de la loi comme étant « un utilisateur qui ne fournit pas de réseau public de communications électroniques ou de services de communications électroniques accessibles au public ».

3. Les données concernées

Les données dont les traitements sont réglementés par les articles 122 et 123 sont les données de trafic et les données de localisation. On le verra, cette distinction a essentiellement pour but de pouvoir définir des règles d'utilisation.

3.1. Les données de trafic

Au sens de l'article 2, 6°, de la loi du 13 juin 2005, on entend par « donnée de trafic », « toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication ».

Les données de trafic sont donc définies par référence aux finalités pour lesquelles elles sont traitées : ce sont toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques (telles que le numéro de téléphone appelant ou appelé, les adresses de courriers électroniques, l'adresse IP de l'expéditeur et du récepteur, etc.) ou pour la facturation de celui-ci (p. ex., pour la durée de la communication, etc.). Elles comprennent les données fournies par l'expéditeur (URL, adresse électronique du destinataire, etc.) ainsi que les données générées par le trafic[1].

3.2. Les données de localisation

La « donnée de localisation » est définie, quant à elle, à l'article 2, 7°, comme « toute donnée traitée dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal[2] d'un utilisateur final d'un service de communications électroniques accessible au public ». Selon les travaux préparatoires de la loi belge, « peuvent constituer une donnée de localisation, la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée »[3].

---

1. Y. Poullet, A. Dix et K. Rosier, « Directive 2002/58/ of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) », *in Concise European IT Law*, 2e éd., Kluwer Law International, 2010, p. 180.
2. Par « équipement terminal », on entend « un produit ou un composant pertinent d'un produit, permettant de réaliser des communications électroniques et destiné à être connecté directement ou indirectement aux interfaces d'un réseau public de communications électroniques » (art. 2, 41°, de la loi du 13 juin 2005).
3. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 73, qui reproduit le texte du considérant 14 de la directive (CE) n° 2002/58.

Il y a lieu de pointer la référence à un service de communications électroniques *accessible au public.* Celle-ci peut paraître incongrue, dès lors qu'on l'a vu, la notion d'opérateur n'est pas exclusivement associée à un réseau de communication accessible au public et que la notion de service de communication accessible au public n'est pas définie. On en retiendra toutefois que, lorsque des données de localisation peuvent être obtenues à propos d'un utilisateur d'un service de communication non accessible au public (p. ex., parce qu'il est lié à un réseau privé d'une entreprise), le traitement de ces données n'est pas réglé par le régime spécifique lié aux données de localisation, mais tomberait sous le champ d'application de la loi du 8 décembre 1992, si les données concernent des personnes physiques.

Par ailleurs, on pourrait penser *a priori* que certaines données de trafic peuvent également être des « données de localisation ».

Les travaux préparatoires semblent toutefois l'exclure : ils précisent qu'il s'agit de données plus précises que les informations relatives au trafic qui sont nécessaires dans les réseaux numériques mobiles pour la transmission de communications[1].

Interprétée telle quelle, la loi belge s'écarte de la compréhension des notions de données de localisation et de données de trafic résultant de la directive (CE) n° 2002/58. En effet, il paraît clair à la lecture des dispositions de la directive qu'une donnée de localisation est une donnée de trafic lorsqu'elle est traitée pour la transmission d'une communication et que son traitement dans ce cadre est régi par les dispositions propres aux traitements de données de trafic[2].

La définition de la notion de donnée de localisation n'est donc pas fonction de la finalité d'utilisation de sorte qu'on peut concevoir qu'il existe des données de localisation non utilisées pour assurer la transmission d'une communication ou la facturation du service. Ce qui importe est que, d'une part, la donnée indique la position géographique d'un terminal et, d'autre part, qu'elle soit traitée « dans un réseau de communications électroniques ou par un service de communications électroniques ». Toutefois, dans le cadre européen, à la différence de celui de la loi belge, une donnée de localisation peut être une donnée de trafic lorsqu'elle est traitée à des fins de transmission ou de facturation. La distinction entre les deux catégories de données ne tient pas à la nature de la donnée, mais vise à permettre de définir des règles différentes suivant l'utilisation qui en est faite. Ainsi, lorsqu'une donnée de localisation est traitée par l'opérateur pour assurer la transmission des communications, elle devra être traitée conformément à l'article 6 de la directive (CE) n° 2002/58 qui concerne le traitement des données de trafic, tandis que, lorsqu'il est question de traiter une donnée de localisation dans un autre but que celui d'assurer la transmission de la com-

1. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 76.
2. Voy. l'article 9 de la directive qui régit le traitement des données de localisation « autres que les données de trafic » ; voy., également, à ce sujet : H. LUTZ et C. HENCKEL, « Data protection and privacy », *in Law and Regulation of Electronic Communication in Europe*, 6e éd., Frankfort, 2013, p. 130.

munication ou sa facturation, ce sont les conditions définies à l'article 9 de la directive relatives au traitement des données de localisation qui sont applicables. Nous verrons qu'en droit belge, on a suivi le même schéma de réglementation nonobstant le fait que la compréhension des notions de données de trafic et de données de localisation semble différente de celle qui est de mise au niveau européen[1].

4. Les finalités de (ré)utilisation permises

4.1. L'acheminement des communications

Aux termes du paragraphe 1er de l'article 122, il est prévu que les opérateurs doivent supprimer les données de trafic concernant les abonnés ou les utilisateurs finals de leurs données de trafic ou rendre ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication.

On en déduit que les opérateurs sont autorisés à traiter les données de trafic dans la mesure où cela est nécessaire pour acheminer la communication. Après la fin de la communication, ils doivent, en revanche, soit les supprimer, soit les rendre anonymes (cette seconde option leur permettant de réaliser, le cas échéant, des statistiques sur l'utilisation de leurs services). À propos du moment où prend fin la communication, les travaux préparatoires de la loi précisent que « [l]e moment exact où s'achève la transmission d'une communication dépend du type de service de communications électroniques fourni. Dans le cas d'un appel d'un service téléphonique public en position déterminée, par exemple, la transmission cesse dès que l'un des utilisateurs finals interrompt la connexion. Dans le cas d'un courrier électronique, la transmission prend fin dès que le destinataire récupère le message auprès de son fournisseur de service »[2].

Il est également précisé dans les travaux préparatoires que « l'obligation d'effacer ou de rendre anonymes les données relatives au trafic lorsqu'elles ne sont plus nécessaires aux fins de la transmission d'une communication n'est pas contradictoire avec les procédures utilisées sur l'Internet, telles que celle de la mise en antémémoire (*caching*), dans le système des noms de domaines pour les adresses IP ou pour les liens entre une adresse IP et une adresse physique, ou l'utilisation d'informations de *login* pour contrôler le droit d'accès à des réseaux ou à des services »[3].

1. Voy. chapitre 5.4, sections 4.3. et 4.4., *infra*.
2. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 73.
3. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 73.

On peut comprendre de ce texte qui s'inspire du considérant 27 de la directive (CE) n° 2002/58, que l'obligation de rendre les données de communications anonymes n'empêchera pas les fournisseurs de services de laisser les technologies visées subsister, quand bien même leur maintien entraînerait la conservation des traces des communications[1]. Cette exception est extrêmement large puisqu'elle autorise cette conservation de données sans limitation de temps, sans garanties et sans droit d'information préalable et d'opposition à celle-ci, sauf à considérer que la loi du 8 décembre 1992 reste totalement applicable à ces traitements[2].

Les opérateurs sont donc censés rendre les données anonymes ou les supprimer, sauf dans la mesure où ils peuvent traiter certaines de ces données à d'autres fins ou qu'ils doivent les conserver ou opérer d'autres traitements dans le cadre d'une collaboration avec des tiers.

Le paragraphe 1er de l'article 122 envisage les obligations de coopération, prévues par ou en vertu de la loi, avec :

- les autorités compétentes pour la recherche ou la poursuite d'infractions pénales ;
- le service de médiation pour les télécommunications pour la recherche de l'identité de toute personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques ;
- les services de renseignement et de sécurité dans le cadre de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Sont visées, sous le couvert de cette exception, non seulement les obligations en matière de rétention[3] pour répondre à des demandes de communication d'information émanant des autorités visées aux points 1° et 3°, mais également une collaboration[4], dans le cadre d'opérations de mise sur écoute à la demande d'un juge d'instruction par exemple[5].

4.2. La facturation des services

Une seconde exception au secret des communications prévue à l'article 112, § 2, est le droit de l'opérateur de stocker et de traiter les informations nécessaires à l'établissement des factures ou pour effectuer les paiements d'interconnexion.

---

1. Cette interprétation semble être confirmée par le commentaire effectué par la Commission à propos de ce considérant 28 dans la Communication de la Commission au Parlement européen (*SEC/2002/0124 final – COD 2000/0189*), selon lequel le « considérant 28 précise encore que certaines formes de stockage de données relatives au trafic, qui sont nécessaires à la fourniture de service sur l'Internet, ne sont pas concernées par l'obligation d'effacer les données relatives au trafic ».
2. J. Dhont et K. Rosier, « Directive vie privée et communications électroniques : premiers commentaires », *R.D.T.I. (ancien-nement revue Ubiquité)*, 2003, p. 37.
3. Voy., à ce propos, le chapitre 5.4, section 4.6., *infra*.
4. Voy. l'article 43*bis* de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.
5. *Cf.* article 88*bis* C. i. cr.

La loi détermine les données pouvant être traitées dans ce cadre et les identifie comme suit :

- l'identification de la ligne appelante ;
- les adresses relatives à l'abonné et au lieu de raccordement, ainsi que le type d'équipement terminal ;
- le nombre total d'unités à facturer pour la période de facturation ;
- l'identification de la ligne appelée ;
- le type d'appel, l'heure à laquelle l'appel a commencé, la durée de l'appel ou la quantité de données transmises ;
- la date de la communication ou du service ;
- d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels.

Dans un avis du 14 juin 2004, la Commission de la protection de la vie privée a souligné qu'il convenait d'interpréter cette disposition comme ne permettant le traitement que des seules données nécessaires à la facturation et/ou, le cas échéant, aux interconnexions, et ce au regard de l'article 6 de la directive (CE) n° 2002/58. Il appartient donc à l'opérateur de déterminer, au cas par cas, et selon les besoins propres au service presté, les données qui, parmi celles figurant sur la liste, sont nécessaires au traitement qu'il met en œuvre[1].

La loi impose également de manière spécifique l'obligation d'information dans ce contexte.
Elle précise :

> « Sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, l'opérateur informe, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent :
> - des types de données de trafic traitées ;
> - des objectifs précis du traitement ;
> - de la durée du traitement. »

Ce texte soulève, à notre sens, plusieurs questions.

Tout d'abord, on peut se demander si l'article 9 de la loi du 8 décembre 1992 qui traite de l'obligation d'information doit être également respecté. Nous sommes d'avis que tel est le cas. Nous renvoyons, à cet égard, à ce qui a été dit dans le chapitre 5.1, section 3, *supra*.

1. C.P.V.P., avis 2004/08 relatif à l'avant-projet de loi relative aux communications électroniques, 14 juin 2004, pp. 4 et 5, www.privacycommission.be.

La seconde question qui nous paraît se poser est celle de la personne à informer. La disposition susmentionnée précise que l'information doit être fournie à l'abonné ou, le cas échéant, à l'utilisateur final. S'agit-il d'un choix laissé à l'opérateur ou doit-on en déduire que cela variera selon les circonstances ? Comme évoqué *supra*[1], il nous paraît que si l'on se réfère à la loi du 8 décembre 1992 qui reste d'application générale et, de ce fait, une référence lorsqu'il s'agit de déterminer les principes en matière de protection des données, il conviendrait de donner la priorité, lorsque cela est possible, à une information donnée à l'utilisateur final personne physique dont les données sont traitées, puisqu'il s'agit de la personne concernée par les données. Ceci dit, il peut s'avérer impossible de fournir, préalablement au traitement, une information à l'utilisateur final soit parce que cette personne n'est pas connue de l'opérateur, sachant que, dans certains cas, il peut y avoir en outre plusieurs utilisateurs (p. ex., plusieurs utilisateurs d'un accès à Internet ou plusieurs personnes qui se servent d'une ligne téléphonique).

Enfin, la loi précise une durée maximale du traitement des données à des fins de facturation jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.

4.3. L'utilisation de données de trafic à des fins de marketing ou de fourniture de services à données de trafic ou de localisation

Une troisième exception au secret des communications, prévue à l'article 122, § 3, permet la réutilisation de données de trafic pour deux finalités différentes : le marketing des services de communication propres à l'opérateur et la fourniture de services à données de trafic ou de localisation.

4.3.1. Les notions de « marketing », de « services à données de trafic » et de « services de localisation »

La notion de marketing n'est pas définie. Cette finalité ne doit toutefois pas permettre la constitution d'un réservoir de données en vue d'un usage à des fins de marketing, de manière générale. En effet, l'article 122, § 3, alinéa 4, évoque plus précisément une action de marketing en spécifiant que le traitement des données doit se limiter aux actes et à la durée nécessaires pour l'action de marketing en question. Il convient de préciser, en outre, que sont seules concernées des opérations de marketing propres à l'opérateur[2]. La loi exclut donc *a priori* l'exploitation de données de localisation pour des actions de marketing relatives à des activités de tiers.

1. Voy. Chapitre 5.1, section 3, *supra*.
2. Voy., sur ce point, C.P.V.P., avis 2004/08 relatif à l'avant-projet de loi relative aux communications électroniques, 14 juin 2004, p. 5, www.privacycommission.be.

Le « service à données de trafic » est défini comme « un service qui exige un traitement particulier des données de trafic allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication »[1]. Le « service à données de localisation » s'entend, quant à lui, d'« un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication »[2].

L'élément clé de ces définitions est donc l'utilisation de données de trafic dans le cadre de la fourniture d'un service distinct de la simple transmission d'une communication. Il est à noter que cette distinction entre services à données de trafic et services à données de localisation n'existe pas dans la directive (CE) n° 2002/58 que transposent notamment les articles 122 et 123 de la loi du 13 juin 2005. Il n'y est question que de « services à valeur ajoutée ». La définition de ce concept prête à discussion parce que l'on doit constater que la version française de la disposition de la directive qui définit cette notion[3] ne correspond pas à la version anglaise[4] et à d'autres versions linguistiques[5].

La loi du 13 juin 2005 adopte des définitions qui empruntent au sens donné à la notion de service à valeur ajoutée telle que reprise dans les autres versions que la version française, en visant un traitement des données allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication. Elle introduit toutefois une distinction entre services selon le type de données traitées, données de trafic ou de localisation. Les travaux préparatoires ne donnent aucune explication sur la raison d'être de cette distinction et ne donnent que des exemples de services que de manière indifférenciée. Selon les travaux préparatoires, de tels services peuvent, par exemple, consister en « la fourniture d'avis relatifs aux ensembles tarifaires les plus intéressants en fonction de l'endroit où l'abonné se trouve, du guidage, des services personnalisés d'information sur la circulation, des bulletins météo ou des informations touristiques »[6].

---

1. Article 2, 8°, de la loi du 13 juin 2005.
2. Article 2, 9°, de la loi du 13 juin 2005.
3. Qui définit le « service à valeur ajoutée » comme « tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation » (art. 2, g, de la directive (CE) n° 2002/58). Cette définition laisse donc entendre que le service à valeur ajoutée implique le traitement des données autres que celles qui ne sont pas indispensables pour la transmission ou la facturation, là où il y aurait lieu d'entendre, selon nous, à l'exclusion de celles qui sont indispensables pour la transmission ou la facturation.
4. Dont le texte est le suivant : « "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof ». (« Un service à valeur ajoutée » s'entend de « tout service qui requiert le traitement de données de trafic ou de localisation autres que des données de trafic au-delà de ce qui est nécessaire pour la transmission d'une communication ou sa facturation » (traduction de l'auteur).)
5. Voy., p. ex., la version néerlandaise dont le texte est le suivant : « "dienst met toegevoegde waarde" : dienst die de verwerking vereist van verkeersgegevens of locatiegegevens anders dan verkeersgegevens, en die verder gaat dan hetgeen nodig is voor het overbrengen van een communicatie of de facturering ervan » (traduction identique à la version anglaise).
6. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 73.

Il convient également de remarquer que cette différenciation entre services à données de localisation ou à données de trafic n'a aucune portée pratique dans la réglementation belge, puisqu'il n'y a pas de réglementation différenciée suivant le type de service fourni, la loi distinguant des régimes différents selon les données traitées (données de trafic ou données de localisation). Il n'y a donc pas de correspondance qui est faite entre données de trafic et service à données de trafic, d'une part, et données de localisation et service à données de localisation, d'autre part. Une donnée de localisation peut être associée à un service à donnée de localisation ou un service à donnée de trafic et il en est de même pour la donnée de trafic.

Cette distinction nous semble donc tout à fait incongrue.

Toujours est-il que pour établir le régime de traitement, il faut se concentrer sur les notions de données de trafic et de données de localisation.

L'article 122, § 3, règle le traitement des données de trafic.

Si l'on schématise la réglementation, on en déduit donc :

- les données de trafic qui sont nécessaires à la transmission ou à la facturation ne peuvent être traitées à des fins de marketing ou dans le cadre d'un service autre que la simple transmission d'une communication qu'à des conditions bien définies et qui seraient précisées à l'article 122, § 3[1] ;
- les données de localisation, qui sont autres que les données de trafic, ne peuvent être traitées dans le cadre d'un service qu'aux conditions définies à l'article 123 de la loi[2].

4.3.2. Les conditions de traitement

Les travaux préparatoires de la loi résument ainsi les exigences imposées par la loi : « Le traitement à des fins de marketing ou pour la fourniture d'un service avec des données relatives au trafic ou de localisation n'est autorisé que si l'abonné ou l'utilisateur final a donné son consentement à cet effet sur la base d'informations précises et complètes de l'opérateur concernant le traitement ultérieur des données qu'il a prévu et sur le droit de l'abonné de ne pas autoriser ce traitement ou de retirer son consentement. Les données relatives au trafic doivent en outre être effacées ou rendues anonymes après la fourniture du service avec des données relatives au trafic ou de localisation »[3].

---

1. L'article 122, § 3, s'inspire d'ailleurs du contenu de l'article 6 de la directive, sauf que les données de trafic telles que comprises dans la directive incluent, le cas échéant, des données de localisation lorsque ces données sont utilisées pour la transmission des communications ou leur facturation.
2. L'article 123 s'inspire d'ailleurs du contenu de l'article 9 de la directive, sauf que la portée de cette disposition est définie comme concernant les données de localisation autres que les données de trafic.
3. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 75.

L'article 122, § 2, précise également que les conditions qui y sont stipulées sont d'application sous réserve des conditions complémentaires découlant de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. On en déduit à nouveau que, pour tout ce qui n'est pas spécifiquement réglé par l'article 122 (telle, p. ex., l'obligation d'information qui y est spécifiquement stipulée), l'opérateur se conforme, le cas échéant, à la loi du 8 décembre 1992 (déclaration préalable, droit d'accès, etc.).

Nous aborderons ces exigences dans l'ordre dans lequel elles sont censées être rencontrées par l'opérateur.

1) L'information préalable

L'opérateur doit, préalablement à la mise en œuvre du traitement, fournir les informations suivantes :

- des types de données de trafic traitées ;
- des objectifs précis du traitement ;
- de la durée du traitement.

Le destinataire de l'information devrait être l'abonné ou, le cas échéant, l'utilisateur final. Nous renvoyons à cet égard ainsi que sur l'application de l'article 9 de la loi du 8 décembre 1992 quant au contenu de l'information à fournir à ce qui a été dit à ce sujet dans le chapitre 5.1, section 3. Liens avec la législation sur la protection des données à caractère personnel., *(supra)*.

2) Le consentement préalable.

L'exploitation des données de trafic par l'opérateur à des fins de marketing ou de fourniture de service à valeur ajoutée est subordonnée à l'obtention du consentement préalable et éclairé de l'abonné ou, le cas échéant, de l'utilisateur final.

Le texte de l'alinéa 2 du paragraphe 2 de l'article 122 précise que, « [p]ar consentement pour le traitement au sens du présent article, on entend la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées ».

Le consentement doit être donné par une personne qui a été dûment informée des utilisations qui seront faites des données. La forme de ce consentement n'est pas précisée. Il est donc envisageable de prévoir la manifestation du consentement par l'activation d'une fonctionnalité qui permet d'avoir accès aux services par exemple.

L'alinéa 3 du paragraphe 3 de l'article 122 exige que ce consentement puisse être retiré à tout moment : l'opérateur concerné doit offrir gratuitement à ses abonnés ou ses utilisateurs finals la possibilité de retirer le consentement donné de manière simple. On voit que les travaux préparatoires ajoutent au texte en stipulant que l'opérateur doit informer l'abonné ou l'utilisateur final de ce qu'il aura le droit de retirer son consentement à tout moment[1].

Sur ce point encore, la loi ne prévoit pas d'exigences quant à la forme dans laquelle ce retrait doit être proposé. On peut donc penser à une possibilité de désactiver une fonctionnalité qui donne accès à un service.

3) La circonscription des actes et de la durée de traitement.

L'alinéa 4 du paragraphe 2 de l'article 122 prévoit que le traitement des données de trafic se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question ou pour l'action de marketing en question.

4.4. L'utilisation de données de localisation à des fins de fourniture de services à données de trafic ou de localisation

Comme nous avons eu l'occasion de le préciser dans la précédente section, le traitement de données de localisation est réglé séparément, à l'article 123 de la loi du 13 juin 2005.

Dans la directive (CE) n° 2002/58, la notion de données de localisation n'est pas exclusive de celle de données de trafic. Des données de localisation sont des données de trafic lorsqu'elles sont utilisées dans la transmission des communications et la facturation des services et, en tant que telles, leurs traitements sont régis par les dispositions applicables aux données de trafic.

Ceci ne semble pas avoir été entériné par la Belgique, et, dans le commentaire dans les travaux préparatoires de ce qui deviendra l'article 123, les données de localisation sont présentées comme des données distinctes des données de trafic[2].

Le régime de l'article 123 se distingue de celui de l'article 122, § 3, sur plusieurs points. Les finalités de traitement sont plus limitées, l'autorisation de traitement est réservée aux opérateurs de réseaux mobiles et certaines conditions de traitement diffèrent. Nous aborderons ces points dans cet ordre.

1. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 75.
2. *Cf.* chapitre 3, section 3.2., *supra*.

4.4.1. Les finalités d'utilisation autorisées

Le paragraphe 1er de l'article 123 précise que les données de localisation se rapportant à un abonné ou un utilisateur final ne peuvent être traitées que lorsqu'elles ont été rendues anonymes ou que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation. Sur ces notions, nous renvoyons au chapitre 5.4, section 3, *supra*. Les travaux préparatoires citent, à titre d'exemple de service fourni grâce à des données de localisation, les services personnalisés d'information sur la circulation[1].

4.4.2. Les opérateurs concernés

L'article 123 s'applique aux opérateurs de réseaux mobiles[2]. Cette notion n'est pas définie dans la loi[3]. Seules le sont celles d'« opérateur » et de « réseaux ». Il nous apparaît toutefois que le réseau mobile se caractérise par le fait que l'abonné ou l'utilisateur n'est pas tenu de se trouver dans un lieu fixe pour bénéficier du service de communication électronique, comme tel est le cas pour l'utilisation de services de téléphonie mobile, de connexion 3G ou 4G pour les *smartphones* ou tablettes ou, encore, de service de guidage par GPS.

4.4.3. Les conditions de traitement

En raison des atteintes potentielles accrues à la vie privée des personnes concernées du fait du risque de les voir localisées à tout moment, le législateur a entendu renforcer les exigences de traitement par rapport à celles imposées pour le traitement des données de trafic. On retrouve, en réalité, les mêmes exigences, sauf en matière d'information qui est plus complète.

1) L'information préalable

L'opérateur doit, préalablement à la mise en œuvre du traitement, fournir les informations suivantes :

- les types de données de localisation traitées ;
- les objectifs précis du traitement ;
- la durée du traitement ;
- les tiers éventuels auxquels ces données seront transmises ;
- la possibilité de retirer à tout moment, définitivement ou temporairement, le consentement donné pour le traitement.

---

1. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 76.
2. Voy., toutefois, les commentaires sur les personnes qui peuvent traiter des données de localisation dans le chapitre 5.4, section 3.2., *infra*.
3. Voy., toutefois, la définition des termes « réseau public de téléphonie mobile » dans l'annexe I de la directive (CE) n° 97/33 du Parlement européen et du Conseil du 30 juin 1997 relative à l'interconnexion dans le secteur des télécommunications en vue d'assurer un service universel et l'interopérabilité par l'application des principes de fourniture d'un réseau ouvert (ONP). Le « réseau public de téléphonie mobile » y est défini comme « un réseau téléphonique public dans lequel les points de terminaison du réseau n'ont pas de position fixe ».

Le destinataire de l'information devrait être l'abonné ou, le cas échéant, l'utilisateur final. Nous renvoyons à cet égard ainsi que sur l'application de l'article 9 de la loi du 8 décembre 1992 quant au contenu de l'information à fournir à ce qui a été dit à ce sujet dans l'Introduction de ce chapitre, section 3. Liens avec la législation sur la protection des données à caractère personnel (*supra*).

2) Le consentement préalable

L'exploitation des données de localisation par l'opérateur à des fins de marketing ou de fourniture de service à valeur ajoutée est subordonnée à l'obtention du consentement préalable et éclairé de l'abonné ou, le cas échéant, de l'utilisateur final.

Le texte de l'article 123 est identique à celui de l'alinéa 2 du paragraphe 2 de l'article 122 sauf en ce qu'il vise un consentement sur le traitement des données de localisation. L'alinéa 4 du paragraphe 2 de l'article 123 exige que ce consentement puisse être retiré à tout moment : l'opérateur concerné doit offrir gratuitement à ses abonnés ou ses utilisateurs finals la possibilité de retirer le consentement donné de manière simple.

Une exception est toutefois prévue à l'exigence du consentement préalable. L'article 123, § 4, stipule qu'« [e]n cas d'appel d'urgence aux centrales de gestion des services d'urgence offrant de l'aide sur place, les opérateurs annulent, pour autant que cela soit techniquement possible, en vue de permettre le traitement de l'appel d'urgence par les centrales de gestion concernées, le refus temporaire ou l'absence de consentement de l'abonné ou de l'utilisateur final concernant le traitement de données de localisation par ligne distincte. Cette annulation est gratuite ».

Ni la forme de ce consentement ni celle du retrait ne sont déterminées. Il est uniquement précisé dans les travaux préparatoires que l'abonné ou l'utilisateur final doit avoir la possibilité de supprimer temporairement, gratuitement et de manière simple, le traitement des données de localisation, sans avoir recours à un courrier recommandé par exemple[1]. Là encore, on peut imaginer que, pour autant que l'utilisateur puisse manifester son retrait de consentement en désactivant une fonctionnalité, pour autant qu'il ait été dûment informé des conséquences d'une telle démarche.

3) La circonscription des actes et de la durée de traitement

À l'instar de ce qui est prévu par l'alinéa 4 du paragraphe 2 de l'article 122, l'article 123, § 2, 3°, impose que le traitement des données de localisation se limite aux actes et à la durée nécessaires pour la finalité autorisée, en l'occurrence la fourniture du service à données de trafic ou de localisation.

---

1. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 76.

4.5. La détection des fraudes

L'article 122, § 4, de la loi prévoit que les données de trafic peuvent être traitées pour déceler des fraudes éventuelles. Il est question, dans les travaux préparatoires, de permettre aux opérateurs d'utiliser les données relatives au trafic qui sont nécessaires pour la facturation en vue de déceler des fraudes, comme le non-paiement pour l'utilisation de services de communications électroniques[1]. La Commission de la protection de la vie privée a, par ailleurs, estimé, dans un avis de 2004, qu'au regard de l'article 15, 1°, de la directive (CE) n° 2002/58, les fraudes visées par la loi ne devraient concerner que des « utilisations non autorisées du système de communications électroniques »[2].

Le texte de la disposition prévoit que les données sont communiquées aux autorités compétentes en cas de délit.

Il est à noter que la disposition légale ne stipule aucune condition spécifique de traitements, de sorte qu'il convient de se reporter à la loi du 8 décembre 1992, notamment en matière d'information.

4.6. La rétention des données de trafic et d'identification

Jusqu'à sa modification par la loi du 30 juillet 2013[3], l'article 126 de la loi du 13 juin 2005 prévoyait :

> « § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre[4] et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue

1. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 75. Ce commentaire est à rapprocher du considérant 29 de la directive (CE) n° 2002/58 qui précise sur ce point que « [d]es données relatives au trafic nécessaires pour la facturation peuvent aussi être traitées par le fournisseur d'un service s'il s'agit de déceler et de faire cesser des pratiques frauduleuses consistant à utiliser le service de communications électroniques sans le payer ».
2. C.P.V.P., avis 2004/08 relatif à l'avant-projet de loi relative aux communications électroniques, 14 juin 2004, p. 6, www.privacycommission.be.
3. Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle.
4. Le terme ministre renvoie aux ministres ou secrétaire d'Etat qui sont compétents pour les matières relatives aux communications électroniques telles que visées dans la présente loi (cf. article 2, 2° de la loi du 13 juin 2005).

de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique. »

Cette disposition imposait donc des traitements de données à l'opérateur consistant en l'enregistrement et la conservation de données, mais les modalités d'exécution de cette disposition devaient être fixées par arrêté royal. Il n'y avait toutefois pas encore eu d'arrêté royal définissant les conditions d'enregistrement et de conservation des données visées adopté à ce jour, nonobstant plusieurs projets établis[1], de sorte que l'article 126 était en pratique inapplicable[2].

Rappelons qu'en vertu de l'article 9, § 7, de la loi du 13 juin 2005, il est prévu qu'un arrêté doit également être pris pour imposer aux fournisseurs et revendeurs de services, dispensés de l'obligation de notification prévue au paragraphe 1er de cette disposition[3], une obligation d'enregistrement et de conservation des données de trafic et d'identification similaire à celle imposée aux opérateurs. De la sorte, certains revendeurs ou fournisseurs (notamment de réseaux privés ne traversant pas le domaine public) qui n'auront pas la qualité d'opérateurs au sens de la loi peuvent se voir néanmoins imposer l'obligation de rétention. L'exécution de cette disposition n'est pas encore intervenue non plus.

L'imposition d'une obligation de conservation des données s'inscrit dans deux bases légales au niveau européen. D'une part, l'article 15 de la directive (CE) n°2002/58 prévoit que les États membres peuvent adopter des mesures législatives visant à limiter la portée de certains des droits et des obligations prévus dans la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou

1. Il y a eu, en effet, plusieurs projets analysés d'ailleurs par la Commission de la protection de la vie privée (avis n° 24/2008 du 2 juillet 2008 relatif à l'avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques et au projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données ; avis 20/2009 relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration, www.privacycommission.be).
2. D. FESLER et E. DEHAFENG, « The Belgian market for electronic communications », *in Law and Regulation of Electronic Communication in Europe*, 6e éd., Frankfort, 2013, p. 265.
3. Voy. les deux catégories de personnes décrites aux paragraphes 5 et 6 de l'article 9 de la loi du 13 juin 2005.

assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. Ces mesures peuvent notamment consister dans l'imposition d'une obligation de conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés ci-avant.

D'autre part, la directive (CE) n° 2006/24 sur la rétention des données régit spécifiquement la problématique des obligations à imposer par les Etats membres aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne[1].

La Belgique a été montrée du doigt par la Commission européenne pour ne pas avoir transposé cette directive, l'article 126 tel que libellé et l'absence d'arrêté d'exécution n'assurant cette transposition[2].

C'est dans ce contexte qu'a été adoptée la loi du 30 juillet 2013 modifiant le libellé de l'article 126 de la loi du 13 juin 2013 comme suit :

> § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic, les données de localisation, les données d'identification d'utilisateurs finals, les données d'identification du service de communications électroniques utilisé et les données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.
>
> Par fournisseurs au sens du présent article, on entend également les revendeurs en nom propre et pour leur propre compte.
>
> Par service de téléphonie au sens du présent article, on entend les appels téléphoniques – notamment les appels vocaux, la messagerie vocale, la téléconfé-

1. *Cf.* article 1er de la directive (CE) n°2006/24.
2. L'absence de transposition complète de la directive a débouché sur une décision du 27 septembre 2012 de la Commission d'adresser une mise en demeure à la Belgique pour défaut de transposition. Pour un commentaire des difficultés rencontrées concernant cette transposition en Belgique, voy. M. VAN BELLINGHEN et T. ZGAJEWSKI, *Les enjeux de la transposition en Belgique des nouvelles directives européennes sur les communications électroniques*, Gand, Academia Press, 2012, p. 40.

rence et la communication de données -, les services supplémentaires – notamment le renvoi ou le transfert d'appels – et les services de messagerie et multimédias, notamment les services de messages brefs (SMS), les services de médias améliorés (EMS) et les services multimédias (MMS).

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de service en application de l'alinéa 1er ainsi que les exigences auxquelles ces données doivent répondre.

Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée.

L'obligation de conserver les données visées à l'alinéa 1er s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :

1° en ce qui concerne les données de la téléphonie, générées, traitées et stockées par les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou

2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.

§ 2. Les données visées au paragraphe 1er, alinéa 1er, sont conservées en vue :
a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46bis et 88bis du Code d'instruction criminelle ;
b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107 ;
c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;
d) de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 1er, alinéa 1er, soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et

toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières.

§ 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées à partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.

Les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises à l'alinéa 1er et celles qui le sont à l'alinéa 2.

§ 4. A la suite du rapport d'évaluation visé au paragraphe 7, le Roi peut, par arrêté délibéré en Conseil des Ministres et après avis de l'Institut et de la Commission de la protection de la vie privée, adapter le délai de conservation des données pour certaines catégories de données, sans ce que ce délai ne puisse dépasser 18 mois.

Le Roi peut, dans les circonstances visées à l'article 4, § 1er, par arrêté délibéré en Conseil des Ministres, et après avis de l'Institut et de la Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à douze mois.

Lorsque, dans les circonstances visées à l'alinéa 2, le Roi fixe un délai de conservation supérieur à vingt-quatre mois, le ministre notifie immédiatement à la Commission européenne et aux autres Etats membres de l'Union européenne toute mesure prise, accompagnée de sa motivation.

§ 5. Pour la conservation des données visées au paragraphe 1er, alinéa 1er, les fournisseurs de réseaux ou de services de communications électroniques visés au paragraphe 1er, alinéa 1er :

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites ;

3° garantissent que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et par les agents et préposés de ces fournisseurs spécifiquement autorisés par ladite Cellule ;

4° veille à ce que les données conservées soient détruites lorsqu'est expiré le délai de conservation applicable à ces données.

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les mesures techniques et administratives que les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, doivent prendre en vue garantir la protection des données à caractère personnel conservées.

Les fournisseurs de services et réseaux visés au paragraphe 1er, alinéa 1er, sont considérés comme responsables du traitement de ces données au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

§ 6. Le ministre et le Ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Commission européenne et à la Chambre des représentants. Ces statistiques comprennent notamment :

1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables ;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, a), seront également jointes au rapport que le Ministre de la Justice doit faire au Parlement conformément à l'article 90decies du Code d'instruction criminelle.

Le Roi détermine, sur proposition du Ministre de la Justice et ministre et sur avis de l'Institut, les statistiques que les fournisseurs de services ou de réseaux transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au Ministre de la Justice.

§ 7. Sans préjudice du rapport visé au paragraphe 6, alinéa 3, le ministre et le Ministre de la Justice font un rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, alinéa 3, sur la mise en œuvre de cet article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation.

Le cadre réglementaire est, au jour où nous rédigeons cette contribution, incomplet puisque l'arrêté royal devant déterminer notamment quelles données doivent être conservées n'a pas encore été adopté.

Sans commenter cette disposition dans le détail[1], on pointera toutefois que l'article 126 étend le champ d'application de l'obligation de conservation à des personnes qui ne sont pas des opérateurs ni même des fournisseurs de services de communication.

L'objectif est d'englober des services relevant de cinq catégories – la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, la messagerie électronique (*e-mail*) et la téléphonie via l'internet-, sans exiger que les prestataires de ces services puissent être qualifiés au regard de la loi du 13 juin 2005 comme des opérateurs ou des fournisseurs de services de communication.

Les travaux préparatoires de la loi précisent à cet égard :

« Le paragraphe 1er vise certaines catégories de fournisseurs de services dont certains sont opérateurs au sens de la loi du 13 juin 2005 relative aux communications électroniques, et d'autres, non, afin d'assurer une transposition correcte de la directive 2006/24/CE.

Ainsi, par exemple, le courrier électronique par l'internet est visé à plusieurs endroits au sein de l'article 5 de la directive. Pour assurer une transposition correcte de cet article de la directive, le paragraphe 1er de l'article 126 inclut également les fournisseurs au public de service de courrier électronique par internet.

1. Un commentaire plus complet sera envisagé dans une prochaine mise à jour.

> Or le courrier électronique par l'internet n'entre pas dans le champ d'application de la définition du service de communications électroniques (art. 2, 5° de la loi du 13 juin 2005) car ce service ne consiste pas à transmettre des signaux mais à fournir, à l'aide de réseaux et services de communications électroniques, du contenu transmis. En incluant les fournisseurs au public de service de courrier électronique par l'internet, le paragraphe 1er de l'article 126 inclut donc des fournisseurs de service qui ne sont pas opérateurs au sens de la loi du 13 juin 2005 relative aux communications électroniques[1] ».

La modification de loi implique que sont désormais tenus de conserver les données les personnes qui fournissent les services de communication électroniques par internet (qui n'assurent pas la transmission de signaux) et plus seulement les fournisseurs les fournisseurs des réseaux publics de communications électroniques sous-jacents, tels que les fournisseur d'accès à internet.

Dans le mêmes temps, certains prestataires de services sont exclus du champ d'application de l'article 126 de la loi. Les fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6 de la loi du 13 juin 2005 relative aux communications électroniques ne sont pas inclus dans le champ d'application du nouvel article 126[2].

4.7. La collaboration avec certaines autorités

Cette obligation de collaboration est abordée dans la loi à l'article 127 et est ainsi circonscrite :

> « § 1er. Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs ou aux utilisateurs finals, en vue de permettre :
>
> 1° l'identification de la ligne appelante dans le cadre d'un appel d'urgence ;
>
> 2° l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'ins-

1. Projet de loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle, *Doc. parl.*, Chambre, Législature n°53, n° 2921/001, p. 12.
2. Projet de loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *Doc. parl.*, Chambre, Législature n°53, n° 2921/001, p. 13. Si, comme expliqué supra, l'article 9, § 7, de la loi du 13 juin 2005 prévoit que ces fournisseurs et revendeurs doivent enregistrer et conserver les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et de la répression d'infractions pénales, et en vue de la répression d'appels malveillants vers les services d'urgence ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organisatrice des services de renseignement et de sécurité, les conditions doivent être fixées par arrêté royal non encore adopté.

truction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Le Roi fixe, après l'avis de l'Institut, la méthode de détermination de la contribution dans les frais d'investissement, d'exploitation et d'entretien de ces mesures qui est à la charge des opérateurs de réseaux et services de communications électroniques, ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées.

§ 2. Sont interdites : la fourniture ou l'utilisation d'un service ou d'un équipement qui rend difficile ou impossible l'exécution des opérations visées au § 1er, à l'exception de systèmes d'encryptage qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements.

§ 3. Jusqu'à ce que les mesures visées au § 1er entrent en vigueur, l'interdiction visée au § 2 ne s'applique pas aux services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.

§ 4. Si un opérateur ne respecte pas les mesures techniques et administratives qui lui sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

§ 5. Les opérateurs déconnectent les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces utilisateurs finals ne sont en aucune manière indemnisés pour la déconnexion.

Si un opérateur ne déconnecte pas les utilisateurs finals qui ne respectent pas les mesures techniques et administratives qui leur sont imposées dans le délai fixé par le Roi, il lui est interdit de fournir le service pour lequel l'utilisateur final n'a pas respecté les mesures qui lui étaient imposées, jusqu'à ce que l'identification de l'appelant ait été rendue possible.

§ 6. Chaque opérateur établit, sur la base du paragraphe 1er, une procédure interne permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition de l'Institut des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse. »

L'article 127 de la loi du 13 juin 2005 impose une obligation de collaboration à l'opérateur. Cette disposition prévoit qu'un arrêté royal devra préciser les obligations qui sont imposées aux opérateurs ou aux utilisateurs finals, en vue de permettre notamment l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de

connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46*bis*, 88*bis* et 90*ter* à 90*decies* du Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité[1].

L'article 9, § 7, de la loi prévoit également l'imposition de l'opération de coopération dans le chef des fournisseurs et revendeurs de services dispensés de l'obligation de notification préalable en application de l'article 9, §§ 5 et 6 (et qui, de ce fait, n'ont pas la qualité d'opérateurs).

Des modalités de collaboration ont été définies dans un arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques[2][3].
Il est toutefois intéressant de pointer un glissement au niveau des personnes tenues par l'obligation de collaboration. En effet, l'arrêté royal du 9 janvier 2003 a défini des obligations dans le chef des « opérateurs de réseaux » et des « fournisseurs de communications électroniques », et non des opérateurs et des personnes visés à l'article 9, § 7. L'explication est à trouver dans le fait que l'arrêté royal vise à porter exécution des articles 46*bis*, § 2, alinéa 1er, 88*bis*, § 2, alinéas 1er et 3, et 90*quater*, § 2, alinéa 3, du Code d'instruction criminelle qui, eux, prévoient la collaboration des opérateurs de réseaux et des fournisseurs de services de communications électroniques[4].

Il convient également de signaler dans ce contexte un arrêt de la Cour de cassation rendu le 18 janvier 2011[5] concernant l'obligation de collaboration qui pouvait être imposée à Yahoo ! Inc. en tant que fournisseur d'un service de messagerie de type *webmail*[6]. La juridiction d'appel avait constaté que Yahoo ! Inc. n'assurait pas elle-même le transport des communications et qu'elle faisait usage de l'infrastructure Web existante et des services de communication existants, de sorte qu'elle ne pouvait être considérée ni comme un opérateur ni comme un fournisseur de communications électroniques.

---

1. Il est à noter que la directive (CE) n° 2002/21 ou « directive-cadre » du Paquet Télécom prévoit, en son considérant 7, que « [l]es dispositions de la présente directive, ainsi que des directives particulières, ne portent pas atteinte à la possibilité dont dispose chaque État membre d'adopter les mesures nécessaires pour garantir la protection de ses intérêts essentiels en matière de sécurité, assurer l'ordre public et la sécurité publique et permettre la recherche, la détection et la poursuite d'infractions pénales, y compris la mise en place par les autorités réglementaires nationales d'obligations spécifiques et proportionnelles applicables aux prestataires de services de communications électroniques ».
2. Tel que modifié par l'arrêté royal du 8 février 2011 modifiant l'arrêté royal du 9 janvier 2003 portant exécution des articles 46*bis*, § 2, alinéa 1er, 88*bis*, § 2, alinéas 1er et 3, et 90*quater*, § 2, alinéa 3, du Code d'instruction criminelle ainsi que de l'article 109*terE*, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Son annexe a été modifiée par l'arrêté royal du 31 janvier 2013 remplaçant l'annexe reprise à l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.
3. Voy., également, l'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité.
4. L'I.B.P.T. présente cet arrêté royal et son annexe comme exécutant l'article 127, § 1er, de la loi du 13 juin 2005 (voy. le document intitulé « La liste des dispositions en vue de l'exécution de la loi du 13 juin 2005 » sur le site www.bitp.be).
5. Cass. (2e ch.), 18 janvier 2011, R.G. n° P.10.1347.N/4.
6. Il est à noter que la Cour de cassation a rendu un deuxième arrêt dans ce même litige le 4 septembre 2012 (R.G. n° P.11.1906.N/3), mais sur une autre question cette fois, à savoir la validité d'une demande écrite visée à l'article 46*bis* du Code d'instruction criminelle, requérant le concours d'un opérateur de réseau de communications électroniques établi en dehors du territoire belge ou du fournisseur d'un service de communications électroniques, faite depuis la Belgique à une adresse établie à l'étranger.

Évoquant le principe de l'autonomie du droit pénal, la Cour a considéré :

> « Le fournisseur d'un service de communications électroniques au sens de l'article 46*bis* du Code d'instruction criminelle n'est pas uniquement l'opérateur belge au sens de la loi du 13 juin 2005 relative aux communications électroniques, mais chacun qui dispense des services de communications électroniques, comme notamment la transmission de données de communication ; l'obligation de concours prévue par l'article 46*bis* du Code d'instruction criminelle ne se limite, dès lors, pas aux opérateurs d'un réseau de communications électroniques ou aux fournisseurs d'un service de communications électroniques qui sont aussi opérateurs au sens de la loi du 13 juin 2005 ou qui ne dispensent leurs services de communications électroniques qu'au moyen de leur propre infrastructure ; cette obligation existe aussi dans le chef de celui qui offre un service qui consiste entièrement ou principalement dans la transmission de signaux par la voie des réseaux de communications électroniques et la personne qui offre un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques »[1].

La Cour de cassation entend donc se fonder sur le fait que l'article 46*bis* du Code d'instruction criminelle a un champ d'application *rationae personae* différent de celui de la loi du 13 juin 2005 (et, à notre sens, plus particulièrement de l'article 127). Elle s'appuie, par ailleurs, sur la notion de fournisseur de service de communication électronique telle que définie dans la loi du 13 juin 2005[2]. Il nous semble dès lors que cela n'implique pas qu'il faille donner un sens différent à la notion de fournisseur de service de communications électroniques en droit pénal, mais simplement avoir égard au fait que le champ d'application de l'article 46*bis* est différent par rapport à d'autres dispositions de la loi du 13 juin 2005[3].

Cet arrêt illustre, à notre estime, les difficultés qui peuvent naître d'une absence de véritable coordination entre les articles 126 et 127 de la loi du 13 juin 2005 et les dispositions du Code d'instruction criminelle précités[4]. Il aurait été évidemment plus clair que l'on trouve dans la loi du 13 juin 2005 des obligations qui concernent les mêmes personnes que celles visées par le Code d'instruction criminelle et l'arrêté

---

1. Pour un commentaire de cette décision, voy., notamment, O. Leroux, « Arnaques, fraudes et escroqueries sur Internet : moyens concrets d'investigation. Point sur l'affaire dite *Yahoo !* à la suite du second arrêt de la Cour de cassation », *J.T.*, 2012, pp. 841 et s., et L. Kerzmann, « L'affaire *Yahoo !* ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle ? », note sous Cass., 18 février 2011, *R.D.T.I.*, 2011, pp. 116 et s.
2. *Cf.* article 2, 5°.
3. Il peut être fait un lien avec l'article 126 de la loi du 13 juin 2005 qui évoque également cette collaboration dont le champ d'application *rationae personae* ne vise pas seulement les personnes visées à l'article 9, § 6 et 127 de la loi du 13 juin 2005. Il permet le traitement des données dans le cadre des obligations de collaboration aux personnes qui seraient tenues d'apporter leur collaboration en application de l'article 46*bis* par exemple.
4. Voy., sur ce point, l'analyse du champ d'application *rationae personae* des différentes dispositions en cause effectuée par la Commission de la protection de la vie privée dans un avis du 3 septembre 2008 (C.P.V.P., avis 29/2008 relatif au projet d'arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, 3 septembre 2008, pp. 4 à 6, www.privacycommission.be).

d'exécution du 9 janvier 2003. Nous avons vu que la donne a été quelque peu modifiée depuis cet arrêt avec la transposition de la directive (CE) n°2006/24 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive (CE) n°2002/58. Dans sa nouvelle mouture[1], l'article 126 impose une obligation de conservation de données à d'autres personnes que les opérateurs ou fournisseurs de services de communications électroniques, et notamment aux fournisseurs de services de courriers électroniques par internet. Nous vous renvoyons aux développements consacrés à cette question dans le chapitre 5.4, section 4.6. *supra*.

5. Qui peut intervenir ou réaliser les opérations de traitement visées aux articles 122 et 123 ?

Les articles 122 et 123 de la loi identifient la personne qui peut, par dérogation au secret des communications électroniques, traiter des données de trafic ou de localisation moyennant le respect de certaines conditions.

5.1. Le traitement des données de trafic

L'article 122 prévoit qu'il s'agit de l'opérateur. En son paragraphe 5, cette disposition prévoit, en outre, que « [l]es données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des clients, de détecter les fraudes, du marketing des services de communications électroniques propres ou de la fourniture de services à données de trafic ou de localisation » et que « [l]e traitement est limité à ce qui est strictement nécessaire à l'exercice de telles activités ».

Les travaux préparatoires indiquent que cette disposition définit de manière limitative les catégories de personnes qui peuvent s'occuper du traitement de données relatives au trafic au sein de la société de l'opérateur[2]. On suppose donc qu'il s'agit ici d'appliquer le principe de l'article 16, § 2, 2°, de la loi du 8 décembre 1992 qui prévoit que le responsable du traitement doit « veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient

1. Cette disposition a été modifiée par l'article 5 de la loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle.
2. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, 2004-2005, n° 1425/001, p. 75.

limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service ». Si tel est le cas, on ne voit pas d'obstacle à ce que l'opérateur puisse, le cas échéant, faire appel, dans le respect des conditions posées à l'article 16 de la loi du 8 décembre 1992, à un sous-traitant pour la réalisation de certaines opérations techniques. La Commission de la protection de la vie privée semble toutefois rejeter cette possibilité en considérant que ce paragraphe exclut en principe la transmission de ces données à d'éventuels sous-traitants (prenant l'exemple de sous-traitants chargés de la récupération de créances)[1]. Ce régime serait donc plus strict que pour le traitement des données de localisation, comme nous le verrons dans la section suivante.

5.2. Le traitement des données de localisation

Contrairement à l'article 122, l'article 123 laisse penser que les données de localisation peuvent être traitées par l'opérateur, mais qu'il pourrait les communiquer à des tiers. L'article 123, § 2, 1°, d), prévoit que l'opérateur doit informer l'abonné ou, le cas échéant, l'utilisateur final des tiers éventuels auxquels les données sont transmises. Dans le cadre de la loi du 8 décembre 1992, le tiers est entendu comme « la personne physique, la personne morale, l'association de fait ou l'administration publique, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ». Si on s'en tient à cette définition, cela impliquerait que les données de localisation pourraient donc être exploitées dans le cadre d'un service à localisation ou à données de trafic par une autre personne que l'opérateur.

Par ailleurs, la Commission de la protection de la vie privée a fait remarquer qu'il se peut que le service à données de localisation soit fourni par un tiers qui n'est pas un fournisseur de services de communications électroniques[2]. La Commission cite l'exemple de GSM proposés actuellement sur le marché et combinés avec un système GPS. Ce type de GSM traite des données de localisation qui pourraient être communiquées directement à un tiers non fournisseur de services à données de localisation, sans que cela passe par un opérateur. Le fournisseur ne serait pas tenu par les obligations définies dans la loi du 13 juin 2005. La Commission en conclut que ce tiers ne serait pas soumis aux exigences de l'article 123 qui ne s'applique qu'aux opérateurs, mais uniquement à la loi du 8 décembre 1992[3].

---

1. C.P.V.P., avis 2004/08 relatif à l'avant-projet de loi relative aux communications électroniques, 14 juin 2004, p. 6, www.privacycommission.be.
2. C.P.V.P., avis n° 18/2007 sur une proposition de loi modifiant la loi relative aux communications électroniques en vue d'assurer une meilleure protection de la vie privée pour les « services à données de localisation » ou services de « géolocalisation » par téléphone portable, 27 avril 2007, p. 4, www.privacycommission.be.
3. Voy., dans le même sens, l'analyse menée par le Groupe de l'article 29 concernant les services de géolocalisation des dispositifs mobiles intelligents (avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, 16 mai 2001, *WP* 185, pp. 4 et s., http ://ec.europa.eu/justice/data-protection/).

En son paragraphe 4, l'article 123 prévoit en outre que « [l]es données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit les données de trafic et de localisation au service. Le traitement est limité à ce qui est strictement nécessaire pour pouvoir fournir au service concerné les données de trafic ou de localisation ». On sous-entend donc que ce n'est pas nécessairement l'opérateur qui détiendrait les données de localisation à l'origine, mais qu'il se peut qu'elles lui soient transmises par un tiers et que, dans ce cas, les données ne peuvent être traitées que par des personnes travaillant sous l'autorité du tiers et dans la mesure strictement nécessaire au service.

6. Les sanctions

La violation des articles 122 et 123 n'est pas en soi sanctionnée pénalement.

Ceci étant, à partir du moment où ces deux dispositions prévoient des exceptions au secret des communications défini à l'article 124 dont le non-respect est sanctionné pénalement, il nous apparaît que des actes de prise de connaissance de données en dehors des conditions prévues par ces deux dispositions pourraient, le cas échéant, constituer une violation de l'article 124, s'ils impliquent la commission d'actes interdits par cette disposition. C'est donc la sanction pénale prévue à l'article 145 de la loi du 13 juin 2005 en cas de violation de l'article 124 qui s'appliquera[1]. De même, un traitement de données opéré sur des données de trafic ou de localisation qui ne respecterait pas la loi du 8 décembre 1992 pourrait être sanctionné sous l'angle de cette loi.

Il est à noter que la violation des articles 126 et 127 est, quant à elle, expressément visée à l'article 145, et sa violation est pénalement sanctionnée comme celle de l'article 124.

1. Voy., sur ce point, le chapitre 5.3, section 5., *supra*.

CHAPITRE 5.5.
LES *COOKIES* ET AUTRES LOGICIELS « ESPIONS »

1. Propos introductifs

L'article 129 de la loi du 13 juin 2005 transpose l'article 5, § 3, de la directive (CE) n° 2002/58.

Cette disposition témoigne d'une reconnaissance explicite du caractère essentiellement privé de l'équipement terminal de l'utilisateur et de l'abonné et des informations qui y sont stockées.

Comme l'affirme le considérant 24 de la directive (CE) n° 2002/58, cet équipement et les informations qui y sont stockées relèvent de la vie privée et doivent être protégés au titre de la Convention européenne des droits de l'homme.

L'article 129 a été modifié par l'article 90 de la loi portant des dispositions diverses en matière de communications électroniques pour transposer les modifications apportées par la directive (CE) n° 2009/136 à l'article 5 de la directive (CE) n° 2002/58.

2. Portée de l'article 129

2.1. Texte légal

L'article 129 est libellé comme suit :

> « Le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur est autorisé uniquement à condition que :
>
> 1° l'abonné ou l'utilisateur concerné reçoive conformément aux conditions fixées dans la loi du 8 décembre 1992 relative à la protection de la vie privée

et à l'égard des traitements de données à caractère personnel, des informations claires et précises concernant les objectifs du traitement et ses droits sur la base de la loi du 8 décembre 1992 ;

2° l'abonné ou l'utilisateur final ait donné son consentement après avoir été informé conformément aux dispositions visées au point 1°.

L'alinéa 1er n'est pas d'application pour l'enregistrement technique des informations ou de l'accès aux informations stockées dans les équipements terminaux d'un abonné ou d'un utilisateur final ayant pour seul but de réaliser l'envoi d'une communication via un réseau de communications électroniques ou de fournir un service demandé expressément par l'abonné ou l'utilisateur final lorsque c'est strictement nécessaire à cet effet.

Le consentement au sens de l'alinéa 1er ou l'application de l'alinéa 2, n'exempte pas le responsable du traitement des obligations de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui ne sont pas imposées par le présent article.

Le responsable du traitement donne gratuitement la possibilité aux abonnés ou utilisateurs finals de retirer le consentement de manière simple. »

2.2. Actes visés

Le principe posé à l'article 129 est celui de l'interdiction du stockage d'informations ou de l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur[1], sauf moyennant le respect des conditions définies par les alinéas 2 et 3 du paragraphe 1er de l'article 129 qui seront analysées *infra*.

L'équipement terminal est défini comme étant « un produit ou un composant pertinent d'un produit, permettant de réaliser des communications électroniques et destiné à être connecté directement ou indirectement aux interfaces d'un réseau public de communications électroniques »[2]. On peut penser à un PC, un GSM, une tablette numérique, etc.

Bien que le texte ne le précise pas expressément, il ressort des travaux préparatoires (qui s'inspirent des considérants de la directive (CE) n° 2002/58[3]) que cette disposition vise à réglementer l'usage de certaines technologies qui permettent de stocker

1. Pour une définition de ces notions, voy. article 2, 11° et 12°, de la loi du 13 juin 2005 ; voy. également chapitre 5.4, section 2.2., *supra*.
2. *Cf.* article 2, 41°, de la loi du 13 juin 2005.
3. Voy. considérant 24 de la directive (CE) n° 2002/58.

ou d'accéder à un équipement terminal à l'insu de l'abonné ou de l'utilisateur, tels les logiciels espions, les pixels invisibles (*web bugs*), les identificateurs cachés et les autres dispositifs analogues qui peuvent pénétrer dans le terminal de l'utilisateur final[1].

Est également visée l'utilisation de *cookies*. Un *cookie* ou « témoin de connexion » est un fichier texte stocké sur le disque dur de l'internaute par le serveur du site Web visité ou par un serveur tiers (tels une régie publicitaire ou un service de Web analytique)[2]. Une fois stockés sur le disque dur d'un internaute, les *cookies* « dialogueront » avec le serveur qui les a placés et renverront à chaque connexion à ce serveur des informations sur les sessions de l'internaute.

Le *cookie* peut créer une intrusion plus ou moins grande suivant le type de données qui sont ainsi renvoyées au serveur qui l'a placé. Dans le considérant 25 de la directive (CE) n° 2002/58, il est de fait réalisé une distinction selon le type de *cookie* utilisé et il est pointé que « les dispositifs de ce type, par exemple des témoins de connexion (*cookies*), peuvent constituer un outil légitime et utile, par exemple pour évaluer l'efficacité de la conception d'un site et de la publicité faite pour ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne. Lorsque des dispositifs du type précité, tels que des témoins de connexion, sont destinés à des fins légitimes, par exemple faciliter la fourniture de services de la société de l'information, leur utilisation devrait être autorisée à condition que les utilisateurs se voient donner des informations claires et précises, conformément à la directive 95/46/CE, sur la finalité des témoins de connexion ou des dispositifs analogues de manière à être au courant des informations placées sur l'équipement terminal qu'ils utilisent ».

Dans un avis du 21 mars 2012, la Commission de la protection de la vie privée livre une analyse plus détaillée des types de témoins de connexion qui existent et préconise un traitement différencié suivant que le *cookie* est destiné à faciliter la navigation (*cookie* de session ou « first party *cookie* » qui retient, par exemple, la langue utilisée par l'internaute lors de sa première connexion à un site) ou qu'il s'agit de traiter des informations plus élaborées sur les préférences de l'internaute pour le profiler (p. ex., concernant un comportement d'achat sur un site de commerce électronique)[3]. Nous y reviendrons à la section suivante.

1. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, sess. 2003-2007, n° 1425-01/1426-01, p. 80.
2. D. Pisscoort, « Publicité et démarchage du consommateur au regard de la protection de la vie privée », *J.T.*, 2012, p. 803.
3. C.P.V.P., avis 10/2012 relatif au projet de loi portant des dispositions diverses en matière de communications électroniques, 21 mars 2012, p. 26, www.privacycommission.be.

2.3. Conditions

2.3.1. Principe : l'exigence d'un consentement informé

L'article 129 autorise l'utilisation des technologies décrites à la section 6.2.2. moyennant obtention du consentement préalable et informé de l'abonné ou de l'utilisateur.

Cela implique une information préalable (1°) et l'obtention d'un consentement (2°).

L'exigence d'un consentement préalable a été introduite par la directive (CE) n° 2009/136 qui a modifié l'article 5, § 3, de la directive 2002/58, transposé à l'article 129. Alors que la directive (CE) n° 2002/56 ne prévoyait qu'une obligation d'information assortie de l'octroi de la possibilité de refuser le placement d'un *cookie*, le texte tel que modifié prévoit désormais l'exigence d'un consentement préalable.

Aux termes de l'alinéa 1er de l'article 129[1], les exigences sont désormais ainsi libellées :

> « 1° l'abonné ou l'utilisateur concerné doit recevoir conformément aux conditions fixées dans la loi du 8 décembre 1992, des informations claires et précises concernant les objectifs du traitement et ses droits sur la base de la loi du 8 décembre 1992.
>
> 2° l'abonné ou l'utilisateur final doit avoir donné son consentement après avoir été informé conformément aux dispositions visées au point 1°. »

Les informations à fournir doivent donc être déterminées par rapport aux exigences de l'article 9 de la loi du 8 décembre 1992 et être fournies par le responsable de traitement. Ainsi, lorsqu'un *cookie* est placé par un tiers par rapport à l'exploitant du site du serveur Web consulté par un internaute (en cas, p. ex., de liens vers des sites publicitaires), ce tiers doit fournir une information sur les traitements qu'il effectue via ce *cookie*, par exemple par le biais d'un hyperlien renvoyant à son propre site[2].

La question de savoir qui de l'abonné ou de l'utilisateur devra recevoir l'information et consentir se pose, à notre sens, dans les mêmes termes que pour les exigences similaires pour d'autres traitements et stipulées aux articles 122, § 3, et 123, § 2, de la loi du 13 juin 2005[3].

---

1. Tel que modifié par l'article 90 de la loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques pour transposer les modifications apportées par la directive (CE) n° 2009/136 à l'article 5 de la directive (CE) n° 2002/58.
2. D. Pissoort, « Publicité et démarchage du consommateur au regard de la protection de la vie privée », *J. T.*, 2012, p. 803.
3. Voy. également, sur ce point, le chapitre 5.1, section 3.

La Commission de la protection de la vie privée s'est toutefois expressément prononcée dans un avis de 2012 sur cette question et a considéré que la personne à informer et qui devait donner son consentement est la personne concernée par le traitement des données au sens de la loi du 8 décembre 1992[1] : lorsque les données traitées concernent un utilisateur final distinct de l'abonné, ce dernier devrait recevoir l'information, le cas échéant en sus de l'abonné[2].

En son alinéa 4, l'article 129 prévoit encore que « [l]e responsable du traitement donne gratuitement la possibilité aux abonnés ou utilisateurs finals de retirer le consentement de manière simple ».

Quant à la technique pour obtenir ce consentement, les travaux préparatoires préconisent l'usage de méthodes pour communiquer des informations ou solliciter le consentement qui soient les plus conviviales possible, par exemple au moyen d'un menu *pop-up* apparaissant avant l'installation des dispositifs[3]. Le considérant 66 de la directive (CE) n° 2009/136 indique que le consentement pourrait valablement être exprimé par la personne par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application. Il est toutefois à noter que la Commission de la protection de la vie privée a exprimé son désaccord avec cette position. Elle estime que le paramétrage des principaux navigateurs étant effectué par défaut comme acceptant les *cookies*, on doit considérer la possibilité d'inférer un consentement de ces paramétrages avec méfiance[4]. Il convient encore de relever que le Groupe de l'article 29 a, en 2011, détaillé différentes manières de solliciter le consentement, outre la fenêtre *pop-up*, en évoquant, par exemple, la possibilité de recourir à un bandeau d'information statique, situé en haut de la page Internet, invitant l'utilisateur à accepter ou refuser l'installation de *cookies*, assorti d'un hyperlien, un écran de démarrage s'affichant lors de l'accès à un site Internet et précisant le type de *cookies* qui seront installés et l'identité des parties qui les installeront si l'utilisateur y consent ou encore un réglage par défaut interdisant le transfert de données à des tiers et invitant l'utilisateur à cliquer pour donner son consentement au transfert à des fins de suivi[5].

1. Voy. article 1er, § 1er, de la loi du 8 décembre 1992.
2. C.P.V.P., avis 10/2012 relatif au projet de loi portant des dispositions diverses en matière de communications électroniques, 21 mars 2012, p. 15, www.privacycommission.be.
3. Projet de loi relative aux communications électroniques, *Doc. parl.*, Chambre, sess. 2003-2007, n° 1425-01/1426-01, p. 80.
4. C.P.V.P., avis 10/2012 relatif au projet de loi portant des dispositions diverses en matière de communications électroniques, 21 mars 2012, p. 15, www.privacycommission.be.
5. Groupe de l'article 29, avis 16/2011 sur le code de bonnes pratiques de l'A.E.E.P. et de l'IAB en matière de publicité comportementale en ligne, 8 décembre 2011, *WP* 188, pp. 10 et s., http ://ec.europa.eu/justice/data-protection/.

2.3.2. Exceptions

L'article 129, alinéa 2, prévoit des exceptions à l'exigence de consentement préalable dans les termes suivants :

« L'alinéa 1er n'est pas d'application pour l'enregistrement technique des informations ou de l'accès aux informations stockées dans les équipements terminaux d'un abonné ou d'un utilisateur final ayant pour seul but de réaliser l'envoi d'une communication via un réseau de communications électroniques ou de fournir un service demandé expressément par l'abonné ou l'utilisateur final lorsque c'est strictement nécessaire à cet effet »[1].

Dans l'avis précité de 2012 qui commentait le projet de loi révisant l'article 129, la Commission de la protection de la vie privée préconisait qu'une liste des *cookies* qui répondent ou non à un des deux critères puisse être établie par la loi (et qui correspondraient aux *cookies* de session ou « first party *cookies* »)[2].

Cette liste n'a pas été établie, mais il existe un avis du Groupe de l'article 29 qui en propose une[3]. Cette liste offre une base de référence utile au responsable du traitement qui place un *cookie* sur un équipement terminal. En effet, ce dernier devra pouvoir justifier, le cas échéant, de l'absence de sollicitation du consentement de l'abonné ou de l'utilisateur sur la base des deux cas de figure envisagés à l'article 129, alinéa 2 : l'envoi de la communication ou la fourniture d'un service de la société de l'information sollicité par l'internaute. D. Pissoort, se fondant sur l'avis du Groupe de l'article 29 dont question ci-avant, cite à titre d'exemples qui pourraient tomber dans ces catégories les *cookies* servant pour les paniers d'achat, des *cookies* servant pour effectuer un *login*, les *cookies* nécessaires à visionner des images ou écouter des sons, à condition dans tous les cas, qu'ils soient supprimés à la fin de la session[4].

2.3.3. Application de la loi du 8 décembre 1992

Aux termes de l'alinéa 3 de l'article 129, il est précisé que « [l]e consentement au sens de l'alinéa 1er ou l'application de l'alinéa 2, n'exempte pas le responsable du

1. Ce texte est légèrement différent de celui de l'article 5, § 3, de la directive (CE) n° 2002/58 tel que modifié par la directive (CE) n° 2009/136 qui dispose que l'exigence de consentement informé « ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur ».
2. C.P.V.P., avis 10/2012 relatif au projet de loi portant des dispositions diverses en matière de communications électroniques, 21 mars 2012, p. 13, www.privacycommission.be.
3. Voy. Groupe de l'article 29, avis 04/2012 sur l'exemption de l'obligation de consentement pour certains *cookies*, 7 juin 2012, http ://ec.europa.eu/justice/data-protection/. Cet avis propose une analyse des deux critères libellés à l'article 5, § 3, de la directive (CE) n°2002/58 tel que modifié par la directive (CE) n° 2009/136. Même si le texte de la directive diffère légèrement de celui de l'article 129, alinéa 2, cette analyse peut se révéler fort utile pour appréhender les différents types de *cookies* existants, outre qu'il fournit une liste de *cookies* qui pourraient être exemptés de l'exigence de consentement.
4. D. Pissoort, « Publicité et démarchage du consommateur au regard de la protection de la vie privée », *J.T.*, 2012, p. 804.

traitement des obligations de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui ne sont pas imposées par le présent article ».

Pour tout ce qui n'est pas spécifiquement réglé par l'article 129, la loi du 8 décembre 1992 reste applicable (durée du traitement, obligation de déclaration, droits d'accès, etc.).

Par ailleurs, dans son avis du 21 mars 2012, la Commission de la protection de la vie privée défend en particulier l'idée selon laquelle les dispositions de la loi du 13 juin 2005 doivent être considérées comme complémentaires à celles de la loi du 8 décembre 1992, mais sans porter préjudice à la loi du 8 décembre 1992. Elle en déduit que l'autorisation de traitement de l'article 129 ne peut faire obstacle à l'exercice du droit d'opposition de la personne concernée à l'utilisation des données à des fins de *marketing direct*, tel que prévu à l'article 12 de la loi du 8 décembre 1992[1].

2.4. Sanctions

Le non-respect de l'article 129 n'est pas spécifiquement sanctionné par la loi du 13 juin 2005.

On pourrait toutefois considérer que, dans la mesure où le traitement de données à caractère personnel interviendrait en contravention avec les conditions prévues à l'article 129, il puisse être sanctionné par le biais de la loi du 8 décembre 1992. En effet, l'article 4, § 1er, de cette loi prévoit que les données doivent être traitées de manière licite et le non-respect de l'article 4 est, quant à lui, pénalement sanctionné à l'article 39, 1°, de cette loi[2].
Par ailleurs, on peut également établir un lien avec les articles 550*bis* et 550*ter* du Code pénal.

L'article 550*bis* du Code pénal érige, en effet, en infraction le fait, sachant qu'on n'y est pas autorisé, d'accéder à un système informatique ou de s'y maintenir. L'article 550*ter* du Code pénal vise, quant à lui, à réprimer le sabotage de données dans un système informatique. En son paragraphe 1er, il sanctionne le fait, sachant que l'on n'y a pas été expressément autorisé, directement ou indirectement, de s'introduire dans un système informatique, de modifier ou d'effacer des données, ou de modifier par tout moyen technologique l'utilisation possible de données dans un système informatique.

1. C.P.V.P., avis 10/2012 relatif au projet de loi portant des dispositions diverses en matière de communications électroniques, 21 mars 2012, p. 4, www.privacycommission.be.
2. Cette disposition prévoit la possibilité d'infliger une amende de 100 à 100 000 euros.

Pour être punissable, il suffit que les actions décrites ci-dessus soient réalisées alors que leur auteur savait qu'il n'y était pas autorisé. L'intention de nuire n'est retenue que pour aggraver la sanction encourue[1].

On peut, dès lors, concevoir que le simple fait d'accéder à un terminal informatique, tel un PC, pour y introduire des données par l'utilisation d'un logiciel espion ou d'accéder à des données pour opérer des modifications à des données qui y sont stockées, et ce, sans le consentement de l'utilisateur, soit constitutif d'une infraction au sens du nouveau paragraphe 1er de l'article 550*ter*.

1. Il est toutefois à noter qu'initialement, l'article 550*ter* requérait que ce sabotage soit réalisé *dans le but de nuire*. À la suite d'une modification du texte introduite par l'article 6 de la loi du 15 mai 2006 modifiant les articles 259*bis*, 314*bis*, 504*quater*, 550*bis* et 550*ter* du Code pénal, le champ d'incrimination de ces infractions est étendu du fait de la suppression de l'exigence d'une intention de nuire.